FortiClient v5.2.1
XML Reference

FortiClient v5.2.1 XML Reference

August 18, 2014

04-521-227660-20140818

Fortinet Document Library	docs.fortinet.com
Fortinet Video Library	video.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2014-08-18	Initial release.

Introduction

FortiClient provides a comprehensive network security solution for endpoints while improving your visibility and control. FortiClient allows you to manage the security of multiple endpoint devices from the FortiGate interface. This document provides an overview of FortiClient v5.2.1 XML configuration.

This document was written for FortiClient (Windows) v5.2.1. Not all features described in this document are supported for FortiClient (Mac OS X) v5.2.1.

For more information on FortiClient installation and configuration, refer to the FortiClient v5.2.1 Administration Guide available at www.FortiClient.com or in the Fortinet Document Library http://docs.fortinet.com.

This document includes the following chapters:

- XML Configuration File
- FortiClient XML Configurations
- Backup or Restore the Configuration File
- Advanced Features

XML Configuration File

FortiClient configuration

File structure

FortiClient supports importation and exportation of its configuration via an XML file. This section defines and describes the format of that file.

File extensions

FortiClient supports the following four file types:

- `.conf`

  A plain-text configuration file.
- `.sconf`

  A secure (encrypted) configuration file.
- `.conn`

  A plain-text VPN connection configuration file.
- `.sconn`

  A secure (encrypted) VPN connection configuration file.

A configuration file can be generated from the settings page of FortiClient dashboard or by using the command-line program: FCConfig.exe, installed with FortiClient. See “Backup or Restore the Configuration File” on page 71 for more information.

Configuration file sections

The configuration file contains the following major sections:

- Meta data

  Basic data controlling the entire configuration file.
- System Settings

  General settings that are not specific to any of the modules listed below (or affects more than one module).
- Endpoint Control

  Endpoint control settings including: enable enforcement, off-net update, skip confirmation, disable unregister, and silent registration.
- VPN

  Global VPN, IPsec VPN, and SSL VPN settings.
- Certificates

  Certificate settings.
- Antivirus

  Antivirus settings including: FortiGuard Analytics, real-time protection, behavior when a virus is detected, and quarantine.

- Single Sign-On Mobility Agent

  Single Sign-On (SSO) mobility agent settings.
- WAN Optimization

  WAN Optimization settings including: HTTP/CIFS/MAPI/FTP support and maximum disk cache size.
- Web Filtering
- Web Filtering settings including: logging, white list priority, maximum violations, rate IP addresses, profiles, Safe Search, and YouTube education filter.
- Application Firewall

  Application Firewall settings.
- Vulnerability Scan

  Vulnerability Scan settings.

Encrypted username and password

Several XML tag elements are named `<password>`. All such tags are always encrypted during configuration exports. For modified and imported configurations, FortiClient accepts either encrypted or plain-text passwords.

Here is an example of an encrypted password tag element. The password starts with *Enc*:

```
<password>Enc9b4e1aae22c65e638aed4e47fbd225256a3b7a24b53f8370d6bc3b9
    aa90cecd5086c995f0549e944b4acc951e4844529c71d81280de2b951</pass
    word>
```

Several `<username>` XML tags also follow this format.

IP addresses

IP address tag elements usually refer to IP version 4 addresses (IPv4). A fully qualified domain name (FQDN) may also be provided. Here are two examples:

- Single IP: `74.196.82.243`
- FQDN: `www.fortinet.com`

Boolean values

Elements that determine if a feature is enabled or disabled use Boolean values. The configuration file accepts `0` for false and `1` for true.

Meta data

All of the XML tags and data in a configuration file are contained inside the XML tag `<forticlient_configuration>`. An empty configuration file will look like this:

```
<?xml version="1.0" encoding="utf-8"?>
<forticlient_configuration>
</forticlient_configuration>
```

The first line of the file includes an XML version number as well as the encoding. This is the standard XML start tag.

The following meta data is supported:

```
<forticlient_version>5.2.1.0602</forticlient_version>
```

FortiClient version number if the file is exported from FortiClient.

```
<version>5.2</version>
```

Version of the configuration file.

```
<date>2014/08/18</date>
```

Date when the file was generated.

```
<partial_configuration>0</partial_configuration>
```

A flag that controls whether the configuration will be replaced or added in import/restore. Possible values are 0 or 1.

```
<os_version>windows</os_version>
```

Indicates whether this configuration is generated from Microsoft Windows or Mac OS X. Possible values are `windows` or `MacOSX`.

System Settings

System settings are contained inside the `<system></system>` XML tags. It includes the following subsections:

- UI settings
- Log settings
- Proxy settings
- Update settings

UI settings

User interface related information are contained inside the <ui></ui> XML tags.

```
<forticlient_configuration>
  <system>
    <ui>
      <ads>0</ads>
      <ads_url></add_url>
      <default_tab>AV</default_tab>
      <flashing_system_tray_icon>1</flashing_system_tray_icon>
      <hide_system_tray_icon>0</hide_system_tray_icon>
      <suppress_admin_prompt>0</suppress_admin_prompt>
      <password>Encrypted/NonEncrypted_PasswordString</password>
      <culture-code>os-default</culture-code>
      <show_passcode>0</show_passcode>
      <gpu_rendering>0</gpu_rendering>
    </ui>
  </system>
</forticlient_configuration>
```

Table 1 provides UI setting XML tags, the description, and the default value (where applicable).

Table 1: UI settings XML tags

XML Tag	Description	Default Value
<ads>	Enable or disable advertisements (Dashboard Banner) in the FortiClient console. Boolean value: [0 | 1]	1
<ads_url>	This field will be removed in future builds.	
<default_tab>	The tab selected by default on the FortiClient dashboard. Type one of the following: • AV: Antivirus • WF: Parental Control/Web Filtering • FW: Application Firewall • VPN: Remote Access • VULN: Vulnerability Scan	AV
<flashing_system_tray_icon>	Enable or disable the flashing system tray icon. The system tray flashes while FortiClient background processes are running. Boolean value: [0 | 1]	1
<hide_system_tray_icon>	Hide or display the system tray icon. Boolean value: [0 | 1]	0
<suppress_admin_prompt>	Do not ask for an administrator password for tasks that require super_user permission to complete. Boolean value: [0 | 1]	0

Table 1: UI settings XML tags (continued)

<password>	Enter a password to set the configuration lock upon registering with a FortiGate. Either encrypted or non-encrypted password. For more information, see "Encrypted username and password" on page 8.	
<culture-code>	The localized language used by the FortiClient dashboard. Type one of the following: • os-default: Defaults to the operating system language • de-de: German • en-us: English (United States) • es-es: Spanish (Spain) • fr-fr: French (France) • ja-jp: Japanese • pt-br: Portuguese (Brazil) • kr-kr: Korean • zh-cn: Chinese (Simplified) • zh-tw: Chinese (Traditional)	os-default
<show_passcode>	Display *Passcode* instead of *Password* in the VPN tab on the FortiClient console. Boolean value: [0 | 1]	0
<gpu_rendering>	Enable or disable GPU rendering. Boolean value: [0 | 1]	0

Log settings

Log-related information will be inside the <log_settings></log_settings> XML tags.

```
<forticlient_configuration>
  <system>
    <log_settings>
      <level>6</level>
      <log_events>ipsecvpn,sslvpn,scheduler,update,firewall,av,clie
          ntmanager,proxy,shield,webfilter,endpoint,fssoma,wanacc,
          configd,vuln</log_events>
      <remote_logging>
        <log_upload_enabled>0</log_upload_enabled>
        <log_upload_server>0.0.0.0</log_upload_server>
        <log_upload_ssl_enabled>1</log_upload_ssl_enabled>
        <log_upload_freq_minutes>90</log_upload_freq_minutes>
        <log_retention_days>90</log_retention_days>
        <log_upload_freq_hours>1</log_upload_freq_hours>
        <log_last_upload_date>0</log_last_upload_date>
        <netlog_categories>7</netlog_categories>
      </remote_logging>
    </log_settings>
  </system>
</forticlient_configuration>
```

Table 2 provides log settings XML tags, the description, and the default value (where applicable).

Table 2: Log settings XML tags

XML Tag	Description	Default Value
<level>	Select the FortiClient logging level. Type one of the following: • 0: emergency • 1: alert • 2: critical • 3: error • 4: warning • 5: notice • 6: information • 7: debug	6

Table 2: Log settings XML tags (continued)

<log_events>	FortiClient events or processes to log. One or more comma-separated list of: • ipsecvpn: IPsec VPN log events • sslvpn: SSL VPN log events • firewall: Application Firewall log events • av: Antivirus log events • webfilter: Web Filtering log events • vuln: Vulnerability Scan log events • wanacc: WAN Optimization log events • fssoma: Single Sign-On (SSO) mobility agent for FortiAuthenticator log events • scheduler: Scheduler log events • update: Update log events • proxy: FortiProxy log events • shield: FortiShield log events • endpoint: Endpoint Control log events • configd: Configuration log events	ipsecvpn,sslvpn,scheduler,update,firewall,av,clientmanager,proxy,shield,webfilter,endpoint,fssoma,wanacc,configd,vuln (enable all events by default)
<remote_logging> elements		
<log_upload_enabled>	Set the boolean value to 1 to upload FortiClient logs to the FortiAnalyzer or FortiManager. Boolean value: [0 | 1]	0
<log_upload_server>	Type the IP address of the FortiAnalyzer or FortiManager to send logs to.	
<log_upload_ssl_enabled>	Enable or disable use of SSL protocol during log upload. Boolean value: [0 | 1]	1
<log_upload_freq_minutes>	The log frequency upload period in minutes.	90
<log_retention_days>	If the server is not reachable, the number of days to retain the logs before being deleted.	90
<log_upload_freq_hours>	Upload frequency interval in hours	1

Table 2: Log settings XML tags (continued)

<log_last_upload_date>	The date of the most recent log upload.	
<netlog_categories>	Type of logs to upload. Bitmask: 1 = traffic logs 2 = vulnerability logs 4 = event logs Since these are bitmasks, you may combine as follows: 3 = 1 or 2 (traffic and vulnerability) 5 = 1 or 4 (traffic and event) 6 = 2 or 4 (vulnerability and event) 7 = 1 or 2 or 4 (all logs)	7

The FortiShield daemon protects FortiClient's own file system and registry settings from modification by unauthorized persons.

Proxy settings

Proxy-related information are contained inside the <proxy></proxy> XML tags. If a proxy server configuration is required for Internet access, use the fields here to specify that configuration so that FortiClient's functions can use Fortinet's Internet based services. The settings are used by FortiClient originated traffic only.

```
<forticlient_configuration>
  <system>
    <proxy>
      <update>0</update>
      <online_scep>0</online_scep>
      <virus_submission>0</virus_submission>
      <type>http</type>
      <address></address>
      <port>80</port>
      <username>Encrypted/NonEncrypted_UsernameString</username>
      <password>Encrypted/NonEncrypted_PasswordString</password>
    </proxy>
  </system>
</forticlient_configuration>
```

Table 3 provides proxy setting XML tags, the description, and the default value (where applicable).

Table 3: Proxy settings XML tags

XML Tag	Description	Default Value
`<update>`	Enable or disable updates. Set the boolean value to `1` if a proxy server exists between FortiClient and the Internet. Boolean value: `[0 | 1]`	`0`
`<online_scep>`	Enable or disable Simple Certificate Enrollment Protocol (SCEP). Set the boolean value to `1` if you are using SCEP server and a proxy server exists between FortiClient and the SCEP server. Boolean value: `[0 | 1]`	`0`
`<virus_submission>`	Enable or disable virus submission to the FortiGuard Distribution Network (FDN). Set the boolean value to `1` if a SMTP proxy server exists between FortiClient and Fortinet's virus submission servers. Used when you *submit for analysis* or *submit as false positive*. Boolean value: `[0 | 1]`	`0`
`<type>`	The type of proxy being specified. Type one of the following: • `HTTP` • `SOCKS4` • `SOCKS5`	`HTTP`
`<address>`	The address of the proxy server. IP address or FQDN.	
`<port>`	The port number of the proxy server. Port range: 1 to 65535	`80`
`<username>`	If the proxy requires authentication, specify the username here. Either encrypted or non-encrypted user name. For more information, see "Encrypted username and password" on page 8.	
`<password>`	If the proxy requires authentication, specify the password here. Either encrypted or non-encrypted password. For more information, see "Encrypted username and password" on page 8.	

Update settings

Update-related information is contained inside the <update></update> XML tags. Use this field to specify how FortiClient performs updates from FortiGuard Distribution Network (FDN) servers.

```
<forticlient_configuration>
  <system>
    <update>
      <use_custom_server>0</use_custom_server>
      <server></server>
      <port>80</port>
      <fail_over_servers>server1.fortinet.com:8008;172.81.30.6:80;s
          erver2.fortinet.com:80</fail_over_servers>
      <timeout>60</timeout>
      <failoverport>8000</failoverport>
      <fail_over_to_fdn>1</fail_over_to_fdn>
      <update_action>notify_only</update_action>
      <scheduled_update>
        <enabled>1</enabled>
        <type>interval</type>
        <daily_at>03:00</daily_at>
        <update_interval_in_hours>3</update_interval_in_hours>
      </scheduled_update>
    </update>
  </system>
</forticlient_configuration>
```

Table 4 provides update setting XML tags, the description, and the default value (where applicable).

Table 4: Update settings XML tags

XML Tag	Description	Default Value
<use_custom_server>	Define a custom server for updates. When the boolean value is set to 0, use the default FDN server address. When the boolean value is set to 1, you must specify the address in <update><server>. Typically used when specifying a FortiManager as your update server. Boolean value: [0 | 1]	0
<server>	IP address or FQDN of the update server. Use when <update><use_custom_server> is set to 1. Optionally, you can specify the port number. Multiple addresses can be specified using a semicolon delimited list. For example, 10.10.10.1:80;10.10.10.2:8080;172.16.10.80;www.myfortimanager.net. If this example, FortiClient will try each server specified in order until one works, or they all fail.	
<port>	Port number of the update server. If a port number is not specified in <update><server>, this port will be used. Port range: 1 to 65535	80

Table 4: Update settings XML tags (continued)

<fail_over_servers>	Update servers to try if the primary server could not be reached. Separate multiple servers with a semicolon. IP address or FQDN, followed by a colon and the port number if applicable.	
<timeout>	Connection timeout, in seconds, when attempting to reach a custom update server. If a server is reachable but not responding to update requests, the actual timeout will be longer. The timeout specified is applied three times to one <server>:<port> pair before FortiClient gives up on this pair. If <failoverport> is specified, and greater than 0, there are a total of six attempts (three attempts for <server>:<port>, three attempts for <server>:<failoverport>).	60
<failoverport>	Failover port number. If the update server cannot be reached via the port specified in <update><server> or <update><port>, FortiClient will try the same address with this port. Port range: 1 to 65535	8000
<fail_over_to_fdn>	Determines whether or not to use FortiGuard servers if communication with custom <server> fails. If the boolean value is set to 1, <update><use_custom_server> is set to 1, and the update server specified by <update><server> cannot be reached, then FortiClient will try the default public FDN server. This is tried only if FortiClient has exhausted all other custom update server options. Boolean value: [0 | 1]	1
<update_action>	Update action applies to software updates only. Select one of the following: • download_and_install: Automatically downloads and installs software updates with no user intervention. It will reboot the computer if needed. • download_only: Automatically downloads software updates, but does not install them. The user can install by following the message prompt. • notify_only: Displays a message when a software update becomes available. The user triggers the update by following the message prompt. • disable: Disables online software updates. Software updates can only be achieved by manually downloading and installing newer installation packages.	notify_only

Table 4: Update settings XML tags (continued)

<scheduled_update> elements Use these elements to define when FortiClient should look for engine, signature and software updates (if enabled).		
<enabled>	Enable or disable scheduled updates. When the boolean value is set to 1, scheduled update is enabled. When set to 0, scheduled update is disabled. Boolean value: [0 | 1]	1
<type>	Update frequency: daily or at regular intervals. Select one of the following: • daily • interval	interval
<daily_at>	Time of the day, in the format HH:MM (24-hour clock), this field is mandatory if the <type> tag is set to daily. This field specifies the time that FortiClient should check for updates.	
<update_interval_in_hours>	Update interval in hours if the <type> tag is set to interval. This field specifies the frequency that FortiClient should check for updates. The minimum value is 1, the maximum value is 24.	3

When <use_custom_server> is 0 or both <server> and <fail_over_servers> are each an empty (NULL) string, FortiClient will only use the default FortiGuard server for software updates. If a string is specified in <server> and communication fails with that server, each of the servers specified in <fail_over_servers> are tried until one succeeds. If that also fails, then software updates will not be possible unless <fail_over_to_fdn> is set to 1.

If communication fails with the server(s) specified in both <server> and <fail_over_servers>, <fail_over_to_fdn> determines the next course of action as listed below:

Table 5: Server XML tag fields

<server>	**<fail_over_to_fdn>**	**Result**
"" (empty strings)	0	Only FortiGuard server is used.
"" (empty strings)	1	Only FortiGuard server is used.
"xyz" (valid IP address)	0	FortiGuard server is never used.
"xyz" (valid IP address)	1	FortiGuard server is used only as failover.

FortiProxy settings

FortiProxy information is contained inside the <fortiproxy></fortiproxy> XML tags. FortiProxy is responsible for HTTP/HTTPS filtering and SMTP/POP3 antivirus scanning. Use these settings to configure FortiProxy's behavior.

```
<forticlient_configuration>
  <system>
    <fortiproxy>
      <enabled>1</enabled>
      <enable_https_proxy>1</enable_https_proxy>
      <http_timeout>60000</http_timeout>
      <client_comforting>
        <pop3_client>1</pop3_client>
        <pop3_server>1</pop3_server>
        <smtp>1</smtp>
      </client_comforting>
      <selftest>
        <enabled>0</enabled>
        <last_port>-172</last_port>
        <notify>0</notify>
      </selftest>
    </fortiproxy>
  </system>
</forticlient_configuration>
```

Table 6 provides FortiProxy XML tags, the description, and the default value (where applicable).

Table 6: FortiProxy XML tags

XML Tag	Description	Default Value
`<enabled>`	Enable or disable FortiProxy. When the boolean value is set to `0`, FortiProxy is disabled. HTTP/HTTPS filtering and SMTP/POP3 antivirus scanning are disabled. Boolean value: `[0 | 1]`	`1`
`<enable_https_proxy>`	Enable or disable HTTPS proxy. When the boolean value is set to `0`, FortiProxy is unable to perform filtering on HTTPS traffic. Boolean value: `[0 | 1]`	`1`
`<http_timeout>`	Connection timeout in seconds. FortiProxy will determine is the remote server is available based on this timeout value. Lower this timeout value if your client requires a faster fail response.	`60`
`<client_comforting> elements` Some types of email clients require continuous response from the server or a connection error may be triggered. Use these settings to enable or disable this feature.		

Table 6: FortiProxy XML tags (continued)

<pop3_client>	Enable or disable POP3 client comforting. Client comforting helps to prevent POP3 clients from complaining that the server has not responded in time. Boolean value: [0 | 1]	1
<pop3_server>	Enable or disable POP3 server comforting. Server comforting helps to prevent POP3 servers from complaining that the client has not responded in time. Example, where FortiClient is installed on a mail server. Boolean value: [0 | 1]	1
<smtp>	Enable or disable SMTP client comforting. SMTP comforting helps to prevent SMTP clients from complaining that the server has not responded in time. Boolean value: [0 | 1]	1
<selftest> elements FortiProxy can detect if other software is disrupting internal traffic between FortiProxy's internal modules. It does this by sending packets periodically to 1.1.1.1, which are intercepted by FortiClient and dropped (they never leave the computer). If the packets are not detected, then it is deemed highly likely that third party software is intercepting the packets, signalling that FortiProxy is not able to perform regular traffic filtering.		
<enabled>	Enable or disable self tests. FortiProxy periodically checks its own connectivity to determine if it is able to proxy other applications traffic. Boolean value: [0 | 1]	1
<last_port>	Last port number used. This is the highest port number you want to allow FortiProxy to listen on. Use to prevent FortiProxy from binding to another port that another service normally uses. Port range: 65535 to 10000	65535
<notify>	When the boolean value is set to 1, the user will see a bubble notification when self-testing detects that HTTP/HTTPS filtering and SMTP/POP3 antivirus scanning have been blocked by a third party program. Boolean value: [0 | 1]	1

Endpoint Control

Endpoint Control configuration elements are usually downloaded from a FortiGate following registration of a FortiClient user to the same FortiGate. There are two sections:

- Endpoint Control general attributes.

  These are contained in the `<endpoint_control></endpoint_control>` XML tags.
- Configuration details relating to specific FortiClient services, such as Antivirus, Web Filtering, Application Firewall, Vulnerability Scanner, and so on. These will be found in the respective configuration elements of the services affected.

Endpoint control general attributes are listed below.

```
<forticlient_configuration>
  <endpoint_control>
    <checksum></checksum>
    <enabled>1</enabled>
    <system_data>Encrypted_String</system_data>
    <socket_connect_timeouts>1:5</socket_connect_timeouts>
    <keepalive_short_timeout>20000</keepalive_short_timeout>
    <keepalive_timeout>1800</keepalive_timeout>
    <custom_ping_server></custom_ping_server>
    <ping_server>172.17.61.178:8010</ping_server>
    <fgt_name>FG_Hostname</fgt_name>
    <fgt_sn>Encrypted_Serial_Number_String</fgt_sn>
    <offnet_update>1</offnet_update>
    <corporate_id>Encrypted_PasswordString<corporate_id>
    <user>Encrypted_UsernameString</user>
    <skip_confirmation>0</skip_confirmation>
    <disable_unregister>0</disable_unregister>
    <fgt_logoff_on_fct_shutdown>1</fgt_logoff_on_fct_shutdown>
    <show_bubble_notifications>0</show_bubble_notifications>
    <conf_recv_time></conf_recv_time>
    <vdom>root</vdom>
    <disable_unregister>0</disable_unregister>
    <silent_registration>0</silent_registration>
    <show_bubble_notifications>1</show_bubble_notifications>
    <fgt_list>Enc256828d1e23febfa0b789324ea1fc9cf45acdc8af3888e7aa2
        6677825bbf8d5d123fcbc2884f3cb3f2a03b5414ab01e6a6c22762add0
        c4f209224f052dec29491e1d15eee4a1a290a81b367c3d4a5251258ed1
        4921e231547f52d9e3</fgt_list>
    <ui>
      <display_antivirus>1</display_antivirus>
      <display_webfilter>1</display_webfilter>
      <display_firewall>1</display_firewall>
      <display_vpn>1</display_vpn>
      <display_vulnerability_scan>1</display_vulnerability_scan>
      <registration_dialog>
        <show_profile_details>1</show_profile_details>
      </registration_dialog>
    </ui>
```

```
      <fortigates>
        <fortigate>
          <serial_number></serial_number>
          <name></name>
          <registration_password></registration_password>
          <addresses></addresses>
        </fortigate>
      </fortigates>
    </endpoint_control>
  </forticlient_configuration>
```

Table 7 provides endpoint control XML tags, the description, and the default value (where applicable).

Table 7: Endpoint control XML tags

XML Tag	Description	Default Value
<checksum>	Configuration checksum calculated on and enforced by the FortiGate.	
<enabled>	Enable endpoint control.	
<system_data>	Endpoint control system information. This element is protected and is not intended to be changed.	
<socket_connect_timeouts>	Probe timeout for endpoint control registration and keep-alive message timeout in seconds. probe_timeout:keep_alive_timeout Changing socket connect time outs might affect performance.	1:5
<keepalive_short_timeout>	Short keepalive timeout in milliseconds (ms).	20000
<keepalive_timeout>	Keepalive timeout in seconds.	1800
<custom_ping_server>	The IP address or FQDN of the custom PING server.	
<ping_server>	The IP address or FQDN of the PING server. FortiClient updates this tag when it registers to the FortiGate. Edits to this tag will be overwritten by FortiClient. This field can be safely deleted.	
<fgt_name>	The name of the FortiGate (FortiGate Hostname) that FortiClient is currently registered to (if any). FortiClient updates this tag when it registers to the FortiGate. Edits to this tag will be overwritten by FortiClient. This field can be safely deleted.	

Table 7: Endpoint control XML tags (continued)

<fgt_sn>	The encrypted serial number of the registered FortiGate (if any). Do not edit this field. This field can be safely deleted.	
<offnet_update>	Enable or disable synchronization of configuration updates from the FortiGate. Boolean value: [0 | 1]	1
<corporate_id>	Encrypted password required to connect to the FortiGate.	
<user>	Encrypted user name.	
<skip_confirmation>	Do not prompt user before proceeding to complete registration with a FortiGate. Boolean value: [0 | 1]	0
<disable_unregister>	Prevent a registered client from being able to unregister after successfully registering to a FortiGate device. Boolean value: [0 | 1] When this setting is configured as 1, the FortiClient user is unable to unregister from the FortiGate after initial registration. This XML setting is intended to be used with <silent_registration>. If *Enable Registration Key for FortiClient* is enabled on the FortiGate, configure this password in the <registration_password> XML tag and enter the IP address or addresses of the FortiGate in the <addresses> XML tag.	0
<fgt_logoff_on_fct_shutdown>	Notify FortiGate when FortiClient is shut down. Boolean value: [0 | 1]	1
<show_bubble_notifications>	Notify the user when new policies are installed. Boolean value: [0 | 1]	1
<conf_recv_time>	Time of the most recently received configuration.	
<vdom>	Name of the FortiGate VDOM that the client is registered to.	
<silent_registration>	Register to the FortiGate without prompting the user to accept registration. When enabled, no end user interaction is required to get the client to register to FortiGate. Boolean value: [0 | 1] This XML setting is intended to be used with <disable_unregister>.	0

Table 7: Endpoint control XML tags (continued)

<show_bubble_notification>	Show notifications in the system tray when a configuration update is received from the FortiGate. Boolean value: [0 | 1]	1
<fgt_list>	Encrypted list of remembered FortiGates. Do not edit this field. This field can be safely deleted.	
<ui> elements		
<display_antivirus>	Display the Antivirus tab in the console. Boolean value: [0 | 1] When this setting is configured as 0, this feature will not be displayed in the FortiClient console.	
<display_webfilter>	Display the Web Filtering tab in the console. Boolean value: [0 | 1] When this setting is configured as 0, this feature will not be displayed in the FortiClient console.	
<display_vpn>	Display the Remote Access (VPN) tab in the console. Boolean value: [0 | 1] When this setting is configured as 0, this feature will not be displayed in the FortiClient console.	
<display_vulnerability_scan>	Display the Vulnerability Scan tab in the console. Boolean value: [0 | 1] When this setting is configured as 0, this feature will not be displayed in the FortiClient console.	
<registration_dialog> element		
<show_profile_details>	Present to user before registration the details of the endpoint profile that will be installed once registration is completed. Boolean value: [0 | 1]	
<fortigates> elements This is a list of FortiGate that will immediately appears in the FortiClient console. The client will be capable of registering with them if they are online. If <endpoint_control><silent_registration> is set to 1 then the client will attempt to silently register. The list is in priority order.		
<fortigate>	This element (with its child elements) should be repeated for each FortiGate that should appear in FortiClient's console interface.	
<serial_number>	[Optional] The serial number of the FortiGate. Displayed to the end user. It may be updated with the real serial number from the FortiGate that the client registers with.	

Table 7: Endpoint control XML tags (continued)

<name>	[Optional] The name of the FortiGate. Displayed to the end user. It may be updated with the real name from the FortiGate that the client registers with.	
<registration_password>	The registration password (encrypted or plain text) required to register to the FortiGates listed in <endpoint_control><fortigates><fortigate><addresses>. If *Enable Registration Key for FortiClient* is enabled on the FortiGate, configure this password in the FortiClient <registration_password> XML setting.	
<addresses>	The FortiGate that appears in the console can be a list of FortiGate addresses. FortiClient will attempt to register to the first FortiGate listed here. A 'redundancy list' of FortiGate IP:port pairs that represent this FortiGate. The list must have at least one FortiGate IP:port pair. Multiple FortiGate IP:port pairs are delimited with a semicolon. Both IP addresses and FQDN are permitted. The list is in priority order. If *Enable Registration Key for FortiClient* is enabled on the FortiGate, configure the IP address or FQDN of the FortiGate in the FortiClient <addresses> XML setting.	

When you disable <ui> elements from being displayed in the FortiClient console, the modules are still installed as part of the FortiClient installation. To configure a VPN only installation, you can use the FortiClient Configurator tool. When selecting VPN only, all other modules are not part of the FortiClient installation.

The <fortigate> element is used to define the FortiGates in a roaming (or redundant) FortiGate configuration. One or more <fortigate> elements may be provided within <fortigates>.

Roaming FortiGate example

In the example below, *Research Lab* and *Fortinet* will appear in FortiClient's console. FortiClient will attempt to register silently to one of the IPs in *Research Lab* first. If both fail (because the laptop is not in the lab), the client will attempt to register to *Fortinet*.

Because *Fortinet* uses a FQDN, the actual FortiGate the client attempts to register to may vary because of DNS settings.

```
<forticlient_configuration>
  <endpoint_control>
    <disable_unregister>1</disable_unregister>
    <silent_registration>1</silent_registration>
    <fortigates>
      <fortigate>
        <name>Research Lab</name>
        <addresses>10.10.10.1:9090;10.10.10.2:9090</addresses>
        <registration_password>33333333</registration_password>
      </fortigate>
      <fortigate>
        <name>Fortinet</name>
        <addresses>fgt.fortinet.com:8002</addresses>
        <registration_password>22222222</registration_password>
      </fortigate>
    </fortigates>
  </endpoint_control>
</forticlient_configuration>
```

The following elements are set by the FortiGate. FortiClient reads them and imports into its configuration when received from the FortiGate. If modified by the user locally on the Windows system, FortiClient will ignore the changes.

```
<vdom>
<disable_unregister>
<ui>
```

For the other elements that could be modified locally, If the same element is received from the FortiGate, the existing value will be overwritten.

The following elements affect Endpoint Control.

Enable or disable display of advertisements.

```
<forticlient_configuration>
  <system>
    <ui>
      <ads>1</ads>
    </ui>
  </system>
</forticlient_configuration>
```

Enable antivirus real-time protection.

```
<forticlient_configuration>
  <antivirus>
    <real_time_protection>
      <enabled>1</enabled>
    <real_time_protection>
  </antivirus>
</forticlient_configuration>
```

Other services that may be configured from the FortiGate will usually use the full set of configuration elements available to them, as described in the various sections of this documents. These include the following:

```
<forticlient_configuration>
  <system>
    <update>
    </update>
    <log_settings>
    </log_settings>
  </system>
  <vpn>
  </vpn>
  <firewall>
  </firewall>
  <webfilter>
  </webfilter>
  <vulnerability_scan>
  </vulnerability_scan>
</forticlient_configuration>
```

VPN

VPN related information is contained inside the `<VPN></VPN>` XML tags. The VPN configuration includes the following subsections:

- VPN options

  Global options that apply to both SSL VPN and IPsec VPN.
- SSL VPN

  SSL VPN related configurations.
- IPsec VPN

  IPsec VPN configurations.

IPsec VPN and SSL VPN each have two subsections:

- Options

  Options related to the specific type of VPN.
- Connections

  User defined connections.

VPN options

The VPN <options> XML tag contains global information controlling VPN states:

```
<forticlient_configuration>
  <vpn>
    <options>
      <current_connection_name>ssldemo</current_connection_name>
      <current_connection_type>ssl</current_connection_type>
      <save_password>0</save_password>
      <autoconnect_tunnel></autoconnect_tunnel>
      <autoconnect_only_when_offnet>0</autoconnect_only_when_offnet
          >
      <keep_running_max_tries>0</keep_running_max_tries>
      <minimize_window_on_connect>1</minimize_window_on_connect>
      <allow_personal_vpns>1</allow_personal_vpns>
      <use_legacy_vpn_before_logon>0</use_legacy_vpn_before_logon>
      <disable_connect_disconnect>0</disable_connect_disconnect>
      <show_vpn_before_logon>0</show_vpn_before_logon>
      <use_windows_credentials>1</use_windows_credentials>
      <show_negotiation_wnd>0</show_negotiation_wnd>
      <diable_dead_gateway_detection>0</diable_dead_gateway_detecti
          on>
      <vendor_id></vendor_id>
    </options>
  </vpn>
</forticlient_configuration>
```

Table 8 provides VPN options XML tags, the description, and the default value (where applicable).

Table 8: VPN options XML tags

XML Tag	Description	Default Value
<current_connection_name>	Name of the current connection, if any.	
<current_connection_type>	Type of the current connection. Select either: [ipsec | ssl]	
<autoconnect_tunnel>	Name of the configured IPsec VPN or SSL VPN tunnel to automatically connect to when FortiClient starts. Requires that the <save_password> tag be set to 1. Boolean value: [0 | 1]	
<autoconnect_only_when_offnet>	Autoconnect only when FortiClient is off-net. Boolean value: [0 | 1]	0
<keep_running_max_tries>	The maximum number of attempts to make when retrying a VPN connection that was lost due to network issues. If this tag is set to 0, it will retry indefinitely.	0

Table 8: VPN options XML tags (continued)

<save_password>	Save user provided connection passwords. Boolean value: [0 | 1]	0
<minimize_window_on_connect>	Minimize the FortiClient dashboard after successfully establishing a connection. Boolean value: [0 | 1]	1
<allow_personal_vpns>	Enable end users to create, modify, and use personal VPN configurations. Boolean value: [0 | 1] When this setting is configured as 0, FortiClient users will not be able to configure personal VPN connections. Only provisioned VPN connections are available to the user.	1
<use_legacy_vpn_before_logon>	Use the old VPN before logon interface. Boolean value: [0 | 1]	1
<disable_connect_disconnect>	Boolean value: [0 | 1]	0
<show_vpn_before_logon>	Allow user to select VPN connection from a list before login onto the system. Boolean value: [0 | 1]	0
<use_windows_credentials>	Connect with the current user name and password. Boolean value: [0 | 1]	1
<show_negotiation_wnd>	Display information on FortiClient dashboard while establishing connections. Boolean value: [0 | 1]	0
<diable_dead_gateway_detection>	Notifies Microsoft Windows OS to disable the detection of dead gateway. You may set this element to 1 if you observe that FortiClient IPsec VPN sends packets using an IP address other than those in the IP address pool assigned by the IPsec VPN server. Boolean value: [0 | 1]	
<vendor_id>	The default value is empty, signifying that FortiClient should use its hard coded ID during IPsec.	

SSL VPN

SSL VPN configurations consist of one `<options>` section, followed by one or more VPN `<connection>` section.

```
<forticlient_configuration>
<vpn>
  <sslvpn>
    <options>
      <enabled>1</enabled>
      <keep_connection_alive>1</keep_connection_alive>
    </options>
    <connections>
      <connection>
        <name>SSLVPN_Name</name>
        <description>Optional_Description</description>
        <server>ssldemo.fortinet.com:10443</server>
        <username>Encrypted/NonEncrypted_UsernameString</username>
        <single_user_mode>0</single_user_mode>
        <ui>
          <show_remember_password>1</show_remember_password>
          <show_alwaysup>1</show_alwaysup>
          <show_autoconnect>1</show_autoconnect>
        </ui>
        <password>Encrypted/NonEncrypted_PasswordString</password>
        <certificate />
        <warn_invalid_server_certificate>1</warn_invalid_server_ce
            rtificate>
        <prompt_certificate>0</prompt_certificate>
        <prompt_username>0</prompt_username>
        <on_connect>
          <script>
            <os>windows</os>
            <script>
              <script>
              <![CDATA[
              net use x: \\server1\share /user:#username#
                   #password#
              net use y: \\server2\share /user:#username#
                   #password#
              net use z: \\server3\share /user:#username#
                   #password#
              copy %temp%\*.logs z:\share\logs\
              copy z:\files\*.* c:\files\
              ]]>
            </script>
          </script>
        </script>
      </on_connect>
      <on_disconnect>
```

```
            <script>
               <os>windows</os>
               <script>
                  <script>
                     <![CDATA[
                     net use x: /DELETE
                     net use y: /DELETE
                     net use z: /DELETE
                     ]]>
                  </script>
               </script>
            </script>
         </on_disconnect>
      </connection>
   </connections>
   </sslvpn>
</vpn>
</forticlient_configuration>
```

Table 9 provides SSL VPN XML tags, the description, and the default value (where applicable).

Table 9: SSL VPN XML tags

XML Tag	Description	Default Value
<sslvpn><options> elements		
<enabled>	Enable or disable SSL VPN. Boolean value: [0 | 1]	1
<keep_connection_alive>	Retry restoring connection of an active VPN session. Boolean value: [0 | 1]	

The <connections> XML tag may contain one or more <connection> elements. Each <connection> has the following:

- information used to establish an SSL VPN connection
- on_connect: a script to run right after a successful connection
- on_disconnect: a script to run just after a disconnection

Connection details is described in table below.

Table 10 provides VPN connection XML tags, the description, and the default value (where applicable).

Table 10:VPN connection XML tags

XML Tag	Description	Default Value
<name>	VPN connection name.	
<description>	Optional description to identify the VPN connection.	

Table 10:VPN connection XML tags (continued)

<server>	IP address or FQDN of SSL server, along with the port number as applicable.	Default port number: 443
<username>	Either encrypted or non-encrypted user name on SSL server. For more information, see "Encrypted username and password" on page 8.	
<single_user_mode>	Enable or disable single user mode. If enabled, new and existing VPN connections cannot be established or will be disconnected if more than one user is logged on the computer Boolean value: [0 | 1]	0
<password>	Either encrypted or non-encrypted password of the given user	
<certificate>	Encrypted certificate name to connect with.	
<warn_invalid_server_certificate>	Enable or disable displaying of a warning message if the server certificate is invalid. Boolean value: [0 | 1]	0
<prompt_certificate>	Request for a certificate during a connection establishment. Boolean value: [0 | 1]	0
<prompt_username>	Request for a user name. Boolean value: [0 | 1]	1
<ui> elements The elements of the <ui> XML tag are set by the FortiGate following an SSL VPN connection.		
<show_remember_password>	Display or hide the remember passwords checkbox in the console. Boolean value: [0 | 1]	
<show_alwaysup>	Display or hide the always up checkbox in the console. Boolean value: [0 | 1]	
<show_autoconnect>	Display or hide the autoconnect checkbox in the console. Boolean value: [0 | 1]	

VPN connection name is mandatory. If a connection of this type and this name exists, its values will be overwritten with the new ones.

The <on_connect> and <on_disconnect> tags both have very similar tag structure:

```
<on_connect>
  <script>
    <os>windows</os>
    <script>
      <script>
        <![CDATA[
        ]]>
      </script>
    </script>
  </script>
</on_connect>
<on_disconnect>
  <script>
    <os>windows</os>
    <script>
      <script>
        <![CDATA[
        ]]>
      </script>
    </script>
  </script>
</on_disconnect>
```

Table 11 provides CDATA XML tags, the description, and the default value (where applicable).

Table 11:CDATA XML tags

XML Tag	Description	Default Value
<os>	The operating system for which the script is written. Select either: [windows | MacOSX]	
<script>	The MS DOS batch or Mac OS X shell script to run.	
<![CDATA[ ]]>	Wraps the scripts in CDATA elements.	
Write MS DOS batch or Mac OS X Shell script inside the CDATA tag. One line per command, just like a regular batch script file. The script will be executed in the context of the user that connected the tunnel. Wherever you write #username# in your script, it will be automatically substituted with the XAuth username of the user that connected the tunnel. Wherever you write #password# in your script, it will be automatically substituted with the XAuth password of the user that connected the tunnel. Remember to check your XML file before deploying to ensure that carriage returns/line feeds are present.		

The example scripts above show a script that mounts several network drives after an SSL connection is established. The drives are unmounted with the corresponding scripts in the <on_disconnect> XML tag.

The <on_connect> and <on_disconnect> scripts are optional.

IPsec VPN

IPsec VPN configurations have one <options> section and one or more <connection> section.

```
<forticlient_configuration>
<vpn>
  <ipsecvpn>
    <options>
      <show_vpn_before_logon>0</show_vpn_before_logon>
      <disconnect_on_log_off>1</disconnect_on_log_off>
      <keep_connection_alive>0</keep_connection_alive>
      <enabled>1</enabled>
      <beep_if_error>0</beep_if_error>
      <beep_continuously>0</beep_continuously>
      <beep_seconds>0</beep_seconds>
      <usewincert>1</usewincert>
      <use_win_current_user_cert>1</use_win_current_user_cert>
      <use_win_local_computer_cert>1</use_win_local_computer_cert>
      <block_ipv6>1</block_ipv6>
      <uselocalcert>0</uselocalcert>
      <usesmcardcert>1</usesmcardcert>
      <enable_udp_checksum>0</enable_udp_checksum>
      <mtu_size>1300</mtu_size>
      <use_windows_credentials>0</use_windows_credentials>
      <disable_default_route>0</disable_default_route>
    </options>
    <connections>
      <connection>
        <name>ipsecdemo</name>
        <single_user_mode>0</single_user_mode>
        <type>manual</type>
        <ui>
          <show_passcode>0</show_passcode>
          <show_remember_password>1</show_remember_password>
          <show_alwaysup>1</show_alwaysup>
          <show_autoconnect>1</show_autoconnect>
        <tray_menu>1</tray_menu>
        <ike_settings>
          <prompt_certificate>0</prompt_certificate>
          <server>ipsecdemo.fortinet.com</server>
          <authentication_method>Preshared
               Key</authentication_method>
          <auth_key>Encdab907ed117eafaadd92f82b3e768b5414e4402dbd4
               df4585d4202c65940f1b2e9</auth_key>
          <mode>aggressive</mode>
          <dhgroup>5;</dhgroup>
          <key_life>28800</key_life>
          <localid></localid>
          <nat_traversal>1</nat_traversal>
```

```
      <mode_config>1</mode_config>
      <enable_local_lan>0</enable_local_lan>
      <nat_alive_freq>5</nat_alive_freq>
      <dpd>1</dpd>
      <dpd_retry_count>3</dpd_retry_count>
      <dpd_retry_interval>5</dpd_retry_interval>
      <enable_ike_fragmentation>0</enable_ike_fragmentation>
      <xauth>
        <enabled>1</enabled>
        <prompt_username>1</prompt_username>
        <username>Encrypted/NonEncrypted_UsernameString</usern
            ame>
        <password />
        <attempts_allowed>1</attempts_allowed>
        <use_otp>0</use_otp>
      </xauth>
      <proposals>
        <proposal>3DES|MD5</proposal>
        <proposal>3DES|SHA1</proposal>
        <proposal>AES128|MD5</proposal>
        <proposal>AES128|SHA1</proposal>
      </proposals>
    </ike_settings>
    <ipsec_settings>
      <remote_networks>
        <network>
          <addr>0.0.0.0</addr>
          <mask>0.0.0.0</mask>
        </network>
      </remote_networks>
      <dhgroup>5</dhgroup>
      <key_life_type>seconds</key_life_type>
      <key_life_seconds>1800</key_life_seconds>
      <key_life_Kbytes>5120</key_life_Kbytes>
      <replay_detection>1</replay_detection>
      <pfs>1</pfs>
      <autokey_keep_alive>0</autokey_keep_alive>
      <use_vip>1</use_vip>
      <virtualip>
        <type>modeconfig</type>
        <ip>0.0.0.0</ip>
        <mask>0.0.0.0</mask>
        <dnsserver>0.0.0.0</dnsserver>
        <winserver>0.0.0.0</winserver>
      </virtualip>
      <proposals>
        <proposal>3DES|MD5</proposal>
        <proposal>3DES|SHA1</proposal>
        <proposal>AES128|MD5</proposal>
```

```
            <proposal>AES128|SHA1</proposal>
          </proposals>
        </ipsec_settings>
        <on_connect>
          <script>
            <os>windows</os>
            <script>
            <script>
              <![CDATA[]]>
            </script>
          </script>
        </script>
      </on_connect>
      <on_disconnect>
        <script>
          <os>windows</os>
          <script>
            <script>
              <![CDATA[]]>
            </script>
          </script>
        </script>
      </on_disconnect>
    </connection>
  </connections>
  </ipsecvpn>
</vpn>
</forticlient_configuration>
```

Table 12 provides IPsec VPN options XML tags, the description, and the default value (where applicable).

Table 12:IPsec VPN options XML tags

XML Tag	Description	Default Value
`<ipsecvpn> <options> elements`		
`<show_vpn_before_logon>`	Display a list of configured VPN tunnels in a list on the Windows logon screen. Boolean value: `[0 | 1]`	`0`
`<disconnect_on_log_off>`	Drop the established VPN connection when the user logs off. Boolean value: `[0 | 1]`	`1`
`<keep_connection_alive>`	Retry restoring the connection of an active VPN session. Boolean value: `[0 | 1]`	`0`
`<enabled>`	Enable or disable IPsec VPN. Boolean value: `[0 | 1]`	`1`

Table 12:IPsec VPN options XML tags (continued)

<beep_if_error>	Beep if VPN connection attempt fails. Boolean value: [0 | 1]	0
<beep_continuously>	Enable or disable the continuous beep. Boolean value: [0 | 1]	1
<beep_seconds>	Type a value for the number of seconds to beep if an error occurs.	60
<usewincert>	Use Microsoft Windows certificates for connections. Boolean value: [0 | 1]	
<use_win_current_user_cert>	Use Microsoft Windows current user certificates for connections. Boolean value: [0 | 1]	1
<use_win_local_computer_cert>	Use Microsoft Windows local computer certificates for connections. Boolean value: [0 | 1]	1
<block_ipv6>	Drop IPv6 traffic when an IPsec VPN connection is established. Boolean value: [0 | 1]	0
<uselocalcert>	Use local certificates for connections. Boolean value: [0 | 1]	
<usesmcardcert>	Use certificates on smart cards. Boolean value: [0 | 1]	
<enable_udp_checksums>	Enable or disable UDP checksums. This setting stops FortiClient from calculating and inserting checksums into the UDP packets that it creates. Boolean value: [0 | 1]	0
<mtu_size>	Maximum Transmit Unit (MTU) size for packets on the VPN tunnel.	
<use_windows_credentials>	Use Microsoft Windows login credentials for VPN authentication. Boolean value: [0 | 1]	
<disable_default_route>	Disable the default route to the gateway when the tunnel is up and restore after the tunnel is down. Boolean value: [0 | 1]	0

The <connections> XML tag may contain one or more <connection> element. Each <connection> has the following:

- name and type: the name and type of connection
- IKE settings: information used to establish an IPsec VPN connection
- IPsec settings:
  - on_connect: a script to run right after a successful connection
  - on_disconnect: a script to run just after a disconnection

Table 13 provides VPN connection XML tags, the description, and the default value (where applicable).

Table 13:VPN connection XML tags

XML Tag	Description	Default Value
<name>	VPN connection name.	
<single_user_mode>	Enable or disable single user mode. If enabled, new and existing VPN connections cannot be established or will be disconnected if more than one user is logged in. Boolean value: [0 | 1]	0
<type>	IPSec VPN connection type. Select either: [manual | auto]	
<tray_menu>	Enable or disable the tray menu. Boolean value: [0 | 1]	1
<ui> elements The elements of the <ui></ui> XML tags are set by the FortiGate following an IPsec VPN connection.		
<show_passcode>	Display *Passcode* instead of *Password* in the VPN tab in the console. Boolean value: [0 | 1]	
<show_remember_password>	Display the remember password checkbox in the console. Boolean value: [0 | 1]	
<show_alwaysup>	Display the always up checkbox in the console. Boolean value: [0 | 1]	
<show_autoconnect>	Display the autoconnect checkbox in the console. Boolean value: [0 | 1]	

The VPN connection name is mandatory. If a connection of this type and this name exists, its values will be overwritten with the new ones.

IKE settings

Internet Key Exchange (IKE) is performed automatically based on pre-shared keys or X.509 digital certificates.

Table 14 provides IKE setting XML tags, the description, and the default value (where applicable).

Table 14:IKE setting XML tags

XML Tag	Description	Default Value
`<prompt_certificate>`	Prompt for certificate on connect. Boolean value: `[0 | 1]`	
`<server>`	IP address or FQDN.	
`<authentication_method>`	Authentication method. Select one of the following: • `Preshared Key` • `X509 Certificate` • `Smartcard X509 Certificate` • `System Store X509 Certificate`	
`<auth_key>`	An encrypted value depending on the authentication method: a preshared key or a certificate name.	
`<mode>`	Connection mode. Select either: `[aggressive | main]`	
`<dhgroup>`	A list of possible Diffie-Hellman (DH) protocol groups, separated by semi-colon.	
`<key_life>`	Phase 2 key expiry duration, in seconds.	`28800`
`<localid>`	Type the peer ID configured in the FortiGate Phase 1 configuration. If *Accept any peer ID* has been configured, leave this field blank.	
`<nat_traversal>`	Enable or disable NAT traversal. Boolean value: `[0 | 1]`	
`<mode_config>`	Enable or disable mode configuration. Boolean value: `[0 | 1]`	
`<enable_local_lan>`	Enable or disable local LAN. Boolean value: `[0 | 1]`	
`<nat_alive_freq>`	NAT alive frequency.	
`<dpd>`	Enable or disable Dead Peer Detection (DPD). Boolean value: `[0 | 1]`	`1`
`<dpd_retry_count>`	Number of times to send unacknowledged DPD messages before declaring peer as dead.	`3`

Table 14:IKE setting XML tags (continued)

<dpd_retry_interval>	Duration of DPD idle periods, in seconds.	5
<enable_ike_fragmentation>	Support fragmented IKE packets.	0
<xauth> elements		
<enabled>	Select to use IKE Extended Authentication (xAuth). Boolean value: [0 | 1]	
<prompt_username>	Request for a user name. Boolean value: [0 | 1]	
<username>	Either encrypted or non-encrypted user name on IPsec server.	
<password>	Either encrypted or non-encrypted password. For more information, see "Encrypted username and password" on page 8.	
<attempts_allowed>	Maximum number of failed login attempts allowed.	
<use_otp>	Use One Time Password (OTP). Boolean value: [0 | 1]	
<proposals> elements		
<proposal>	Encryption and authentication types to use, separated by a pipe. Example: <proposal>3DES|MD5<proposal> Multiple elements accepted. First setting: Encryption type: DES, 3DES, AES128, AES192, AES256 Second setting: Authentication type: MD5, SHA1, SHA256, SHA384, SHA512	

IPsec settings

Table 15 provides IPsec settings XML tags, the description, and the default value (where applicable).

Table 15:IPsec setting XML tags

XML Tag	Description	Default Value
<remote_networks> elements		
<network>	Specifies a network address <addr> with subnet mask <mask>.	
<addr>	Network IP address.	
<mask>	Subnet mask to apply to network address <addr>.	

Table 15:IPsec setting XML tags (continued)

<dhgroup>	A list of possible Diffie-Hellman (DH) protocol groups, separated by semi-colon.	
<key_life_type>	Phase 2 key re-key duration type. Select one of the following: • seconds • kbytes • both	
<key_life_seconds>	Phase 2 key maximum life in seconds.	1800
<key_life_Kbytes>	Phase 2 key maximum life in kB.	5120
<replay_detection>	Detect an attempt to replay a previous VPN session.	
<pfs>	Enable or disable Perfect Forward Secrecy (PFS). Boolean value: [0 | 1]	
<autokey_keep_alive>	Enable or disable autokey keep alive. Boolean value: [0 | 1]	
<use_vip>	Use virtual IP. Boolean value: [0 | 1]	
<virtualip> elements		
<type>	Type of virtual IP. Select either: [modeconfig | dhcpoveripsec]	
<ip>	IP address.	
<mask>	Network mask.	
<dnsserver>	DNS server IP address.	
<winserver>	Microsoft Windows server IP address.	
<proposals> elements		
<proposal>	Encryption and authentication types to use, separated by a pipe. Example: <proposal>3DES|MD5<proposal> Multiple elements accepted. First setting: Encryption type: DES, 3DES, AES128, AES192, AES256 Second setting: Authentication type: MD5, SHA1, SHA256, SHA384, SHA512	

The on_connect and on_disconnect structure and scripting format are similar to that described in the section titled: SSL VPN earlier.

Certificates

Certificates are contained in the <certificates></certificates> XML tags. There are two subsections:

- CA certificate

  Base 64 encoded CA certificate.
- CRL

  Uses Online Certificate Status Protocol (OCSP).

```
<forticlient_configuration>
  <certicates>
  <CA_certificates/>
    <CRL>
      <OCSP>
        <enabled>1</enabled>
        <server>187.205.34.96</server>
        <port>80</port>
      </OCSP>
    </CRL>
  </certficates>
</forticlient_configuration>
```

Table 16 provides certificate XML tags, the description, and the default value (where applicable).

Table 16: Certificate XML tags

XML Tag	Description	Default Value
<CRL><OCSP> elements		
<enabled>	Use Online Certificate Status Protocol (OCSP). Boolean value: [0 | 1]	
<server>	Type the server IP address.	
<port>	Type the server port number.	

Antivirus

The Antivirus configuration data are contained in the `<antivirus></antivirus>` XML tags.

The following are subsections of the antivirus configuration.

- General options
  Options that apply to the overall operation of the antivirus service.
- Scheduled scans
  Scheduled scanning of the system.
- On-demand scans
  Details relating to on-demand scans.
- Real-time protection
  Options to use during when real-time protection scanning is activated.
- Email
  How to handle scanning of email messages.
- Quarantine
  Configures quarantine operations.
- Server
  Special options for servers.

Antivirus general options

This has options that enable or disable various services in the antivirus feature.

```
<forticlient_configuration>
  <antivirus>
    <enabled>1</enabled>
    <signature_expired_notification>0</signature_expired_notificati
        on>
    <scan_on_insertion>0</scan_on_insertion>
    <shell_integration>1</shell_integration>
    <antirootkit>4294967295</antirootkit>
    <fortiguard_analytics>0</fortiguard_analytics>
    <multi_process_limit>0</multi_process_limit>
  </antivirus>
</forticlient_configuration>
```

Table 17 provides antivirus general option XML tags, the description, and the default value (where applicable).

Table 17: Antivirus general option XML tags

XML Tag	Description	Default Value
`<enabled>`	Enable or disable antivirus. Boolean value: `[0 | 1]`	`1`
`<signature_expired_notification>`	Enable or disable expired signature notification. Boolean value: `[0 | 1]`	`0`

Table 17: Antivirus general option XML tags (continued)

<scan_on_insertion>	Enable or disable scan on insertion. Boolean value: [0 | 1]	0
<shell_integration>	Enable or disable shell integration. Boolean value: [0 | 1]	1
<antirootkit>	Enable or disable antirootkit. This field is a bit mask. When set to 0, all antirootkit features are disabled. 4294947295 (=0xffffffff) means all antirootkit features are enabled.	
<fortiguard_analytics>	Enable or disable FortiGuard Analytics. Boolean value: [0 | 1]	1
<multi_process_limit>	The number of antivirus scanning processes to use for scheduled or on-demand scans. The maximum is the number of CPU processors and cores. When set to 0, FortiClient will determine the optimal value.	0

Scheduled scans

User may schedule scanning for viruses in one of three ways:

- Full scan

  Scan the entire system.
- Quick scan

  Scan only none-system files.
- Custom scan

  Scan a selection of files, as specified by user.

Zero, one or more of these may be configured at any one time.

```
<forticlient_configuration>
  <antivirus>
    <scheduled_scans>
      <quick>
        <enabled>1</enabled>
        <repeat>1</repeat>
        <date>2013/10/02</date>
        <days>2</days>
        <day_of_month>21</day_of_month>
        <time>15:30</time>
      </quick>
      <full>
        <enabled>1</enabled>
        <repeat>1</repeat>
        <days>2</days>
        <time>18:30</time>
```

```
            <removable_media>1</removable_media>
            <network_drives>0</network_drives>
            <priority>0</priority>
          </full>
          <directory>
            <enabled>1</enabled>
            <repeat>1</repeat>
            <date>2013/10/02</date>
            <days>2</days>
            <day_of_month>21</day_of_month>
            <time>18:30</time>
            <directory>c:\users\</directory>
            <priority>2</priority>
          </directory>
        </scheduled_scans>
      </antivirus>
    </forticlient_configuration>
```

Each of three scheduling options require specification of several common elements, which define when scanning should occur. The common elements are described first. Other elements specific to the full and custom scans are described later.

Table 18 provides scheduled scan XML tags, the description, and the default value (where applicable).

Table 18: Scheduled scan XML tags

XML Tag	Description	Default Value
common elements		
<enabled>	Enable or disable scheduled scan. Boolean value: [0 | 1]	
<repeat>	Frequency of scans. Select one of the following: • 0: daily • 1: weekly • 2: monthly	
<date>	Date to run scan in the format YYYY/MM/DD.	
<days>	Day of the week to run scan. Multiple days may be provided, separated by comma. Select one or more of the following: • 1: Sunday • 2: Monday • 3: Tuesday • 4: Wednesday • 5: Thursday • 6: Friday • 7: Saturday	

Table 18: Scheduled scan XML tags (continued)

<day_of_month>	The day of the month to run a scan. A number from 1 to 31.	
<time>	Time value in 24 hour clock.	

Only one of the elements: <date>, <days>, <day_of_month> is required. The factory default at the time of installation is to run a full scan on Mondays at 18:30 hours.

Table 19 provides element XML tags, the description, and the default value (where applicable).

Table 19: Element XML tags

XML Tag	Description	Default Value
<full> elements		
<removable_media>	Enable or disable scanning files on removable media. Boolean value: [0 | 1]	1
<network_drives>	Enable or disable scanning files on network drives. Boolean value: [0 | 1]	0
<priority>	Scan priority. Select one of the following: • 0: normal • 1: low • 2: high	0
<directory> elements		
<directory>	The full path to the directory to scan.	
<priority>	Scan priority. Select one of the following: • 0: normal • 1: low • 2: high	

On-Demand scans

The <on_demand_scanning> element defines how the antivirus scanner handles scanning of files manually requested by the end user.

```
<forticlient_configuration>
  <antivirus>
    <on_demand_scanning>
    <use_extreme_db>1</use_extreme_db>
    <on_virus_found>4</on_virus_found>
    <pause_on_battery_power>1</pause_on_battery_power>
    <automatic_virus_submission>
      <enabled>0</enabled>
      <smtp_server>fortinetvirussubmit.com</smtp_server>
      <username />
```

```
        <password>Encrypted/NonEncrypted_PasswordString</password>
      </automatic_virus_submission>
      <compressed_files>
        <scan>1</scan>
        <maxsize>0</maxsize>
      </compressed_files>
      <riskware>
        <enabled>1</enabled>
      </riskware>
      <adware>
        <enabled>1</enabled>
      </adware>
      <heuristic_scanning>1</heuristic_scanning>
      <scan_file_types>
        <all_files>1</all_files>
        <file_types>
          <extensions>.386,.ACE,.ACM,.ACV,.ACX,.ADT,.APP,.ASD,.ASP,.
              ASX,.AVB,.AX,.AX2,.BAT,.BIN,.BTM,.CDR,.CFM,.CHM,.CLA,.
              CLASS,.CMD,.CNN,.COM,.CPL,.CPT,.CPY,.CSC,.CSH,.CSS,.DE
              V,.DLL,.DOC,.DOT,.DRV,.DVB,.DWG,.EML,.EXE,.FON,.GMS,.G
              VB,.HLP,.HTA,.HTM,.HTML,.HTT,.HTW,.HTX,.HXS,.INF,.INI,
              .JPG,.JS,.JTD,.KSE,.LGP,.LIB,.LNK,.MDB,.MHT,.MHTM,.MHT
              ML,.MOD,.MPD,.MPP,.MPT,.MRC,.OCX,.PIF,.PL,.PLG,.PM,.PN
              F,.PNP,.POT,.PPA,.PPS,.PPT,.PRC,.PWZ,.QLB,.QPW,.REG,.R
              TF,.SBF,.SCR,.SCT,.SH,.SHB,.SHS,.SHT,.SHTML,.SHW,.SIS,
              .SMM,.SWF,.SYS,.TD0,.TLB,.TSK,.TSP,.TT6,.VBA,.VBE,.VBS
              ,.VBX,.VOM,.VSD,.VSS,.VST,.VWP,.VXD,.VXE,.WBK,.WBT,.WI
              Z,.WK,.WML,.WPC,.WPD,.WSC,.WSF,.WSH,.XLS,.XML,.XTP</ex
              tensions>
            <include_files_with_no_extension>0</include_files_with_n
                o_extension>
        </file_types>
        </scan_file_types>
        <exclusions>
        <file></file>
        <folder></folder>
        <file_types>
          <extensions></extensions>
        </file_types>
      </exclusions>
      </on_demand_scanning>
    </antivirus>
</forticlient_configuration>
```

Table 20 provides on-demand scan XML tags, the description, and the default value (where applicable).

Table 20: On-demand scan XML tags

XML Tag	Description	Default Value
<use_extreme_db>	Use the extreme database. Boolean value: [0 | 1]	1
<on_virus_found>	The action FortiClient will perform if a virus is found. Select one of the following: • 0: clean • 1: ignore • 2: repair • 3: warning • 4: quarantine • 5: deny access	4
<pause_on_battery_power>	Suspend scanning when system is on battery. Boolean value: [0 | 1]	1
<heuristic_scanning>	Enable or disable heuristics signatures. Boolean value: [0 | 1]	1
<automatic_virus_submission> elements		
<enabled>	Send virus files found to FortiGuard servers. Boolean value: [0 | 1]	0
<smtp_server>	SMTP server IP address or FQDN.	fortinetvirussubmit.com
<password>	Either encrypted or non-encrypted password. For more information, see “Encrypted username and password” on page 8.	
<compressed_files> elements		
<scan>	Enable or disable scanning of compressed files. Boolean value: [0 | 1]	1
<maxsize>	Maximum compressed file size to scan in MB. A number up to 65535. 0 means no limit.	0
<riskware> elements		
<enabled>	Enable or disable scanning of riskware files. Boolean value: [0 | 1]	1
<adware> element		

Table 20: On-demand scan XML tags (continued)

<enabled>	Enable or disable scanning of adware files. Boolean value: [0 | 1]	1
<scan_file_types> element		
<all_files>	Enabled or disable scanning of all file types. If enabled, ignore the <file_types> element. Boolean value: [0 | 1]	1
<scan_file_types> <file_types> elements		
<extensions>	Comma separated list of extensions to scan.	
<include_files_with_no_extension>	Determines whether to scan files with no extension. Boolean value: [0 | 1]	0
<exclusions> elements		
<file>	Full path to a file to exclude from on-demand scanning. Wildcards are not accepted. Element may be repeated to list more files.	
<folder>	Full path to a directory to exclude from on-demand scanning. Wildcards are not accepted. Element may be repeated to list more directories.	
<exclusions> <file_types> element		
<extensions>	Comma separated list of extensions to exclude from on-demand scanning.	

Real-time protection

The <real_time_protection> element configures how the scanner processes files used by programs running on the system.

Several tags are similar between this section and the previous one: <on_demand_scanning>.

```
<forticlient_configuration>
  <antivirus>
    <real_time_protection>
      <enabled>1</enabled>
      <use_extreme_db>0</use_extreme_db>
      <when>0</when>
      <ignore_system_when>0</ignore_system_when>
      <on_virus_found>0</on_virus_found>
      <popup_alerts>0</popup_alerts>
      <popup_registry_alerts>0</popup_registry_alerts>
      <cloud_based_detection>
        <on_virus_found></on_virus_found>
      </cloud_based_detection>
```

```
            <compressed_files>
              <scan>1</scan>
              <maxsize>2</maxsize>
            </compressed_files>
            <riskware>
              <enabled>1</enabled>
            </riskware>
            <adware>
              <enabled>1</enabled>
            </adware>
            <heuristic_scanning>
              <level>1</level>
              <enabled>0</enabled>
              <action>0</action>
            </heuristic_scanning>
            <scan_file_types>
              <all_files>1</all_files>
              <file_types>
              <extensions>.386,.ACE,.ACM,.ACV,.ACX,.ADT,.APP,.ASD,.ASP,.
                   ASX,.AVB,.AX,.AX2,.BAT,.BIN,.BTM,.CDR,.CFM,.CHM,.CLA,.
                   CLASS,.CMD,.CNN,.COM,.CPL,.CPT,.CPY,.CSC,.CSH,.CSS,.DE
                   V,.DLL,.DOC,.DOT,.DRV,.DVB,.DWG,.EML,.EXE,.FON,.GMS,.G
                   VB,.HLP,.HTA,.HTM,.HTML,.HTT,.HTW,.HTX,.HXS,.INF,.INI,
                   .JPG,.JS,.JTD,.KSE,.LGP,.LIB,.LNK,.MDB,.MHT,.MHTM,.MHT
                   ML,.MOD,.MPD,.MPP,.MPT,.MRC,.OCX,.PIF,.PL,.PLG,.PM,.PN
                   F,.PNP,.POT,.PPA,.PPS,.PPT,.PRC,.PWZ,.QLB,.QPW,.REG,.R
                   TF,.SBF,.SCR,.SCT,.SH,.SHB,.SHS,.SHT,.SHTML,.SHW,.SIS,
                   .SMM,.SWF,.SYS,.TD0,.TLB,.TSK,.TSP,.TT6,.VBA,.VBE,.VBS
                   ,.VBX,.VOM,.VSD,.VSS,.VST,.VWP,.VXD,.VXE,.WBK,.WBT,.WI
                   Z,.WK,.WML,.WPC,.WPD,.WSC,.WSF,.WSH,.XLS,.XML,.XTP</ex
                   tensions>
              <include_files_with_no_extension>0</include_files_with_no_
                   extension>
              </file_types>
            </scan_file_types>
            <exclusions>
              <file_types>
                <extensions />
              </file_types>
            </exclusions>
          </real_time_protection>
          </antivirus>
        </forticlient_configuration>
```

Table 21 provides real time protection XML tags, the description, and the default value (where applicable).

Table 21: Real time protection XML tags

XML Tag	Description	Default Value
<enabled>	Enable or disable real time protection. Boolean value: [0 | 1]	1
<use_extreme_db>	Use extreme database. Boolean value: [0 | 1]	
<when>	File I/O activities that result in a scan. Select one of the following: • 0: read and write • 1: only on read • 2: only on write	0
<ignore_system_when>	Boolean value: [0 | 1]	0
<on_virus_found>	The action FortiClient will perform if a virus is found. Select one of the following: • 0: clean • 1: ignore • 2: repair • 3: warning • 4: quarantine • 5: deny access	5
<popup_alerts>	Display alerts when a virus is found. Boolean value: [0 | 1]	1
<popup_registry_alerts>	Enable or disable pop-up registry alerts. This feature displays alerts if a process tries to change registry start items. Boolean value: [0 | 1]	0
<cloud_based_detection> elements		
<on_virus_found>	The action FortiClient will perform when a virus is detected by the Cloud Based Behavior Scan (CBBS). Select one of the following: • 0: Clean • 1: Ignore • 2: Repair • 3: Warning • 4: Quarantine • 5: Deny access	
<compressed_files> elements		

Table 21: Real time protection XML tags (continued)

<scan>	Enable or disable scanning of compressed files. Boolean value: [0 | 1]	1
<maxsize>	Maximum compressed file size to scan in MB. A number up to 65535. 0 means no limit.	2
<riskware> element		
<enabled>	Enable or disable scanning of riskware files. Boolean value: [0 | 1]	1
<adware> element		
<enabled>	Enable or disable scanning of adware files. Boolean value: [0 | 1]	1
<heuristic_scanning> elements		
<level>	Level is from 0 to 3. Applied to both real-time and on-demand scans.	
<enabled>	Enable or disable heuristics signatures. Boolean value: [0 | 1]	0
<action>	The action FortiClient will perform if a virus is found. Select either: • 0: warning • 1: deny access	
<scan_file_types> element		
<all_files>	Enabled or disable scanning of all file types. If enabled, ignore the <file_types> element. Boolean value: [0 | 1]	1
<scan_file_types><file_types> elements		
<extensions>	Comma separated list of extensions to scan.	
<include_files_with_no_extension>	Determines whether to scan files with no extension. Boolean value: [0 | 1]	0
<exclusions> elements		
<file>	Full path to a file to exclude from on-demand scanning. Wildcards are not accepted. Element may be repeated to list more files.	
<folder>	Full path to a directory to exclude from on-demand scanning. Wildcards are not accepted. Element may be repeated to list more directories.	

Table 21: Real time protection XML tags (continued)

<exclusions> <file_types> element		
<extensions>	Comma separated list of extensions to exclude from on-demand scanning.	

Email

Emails will be scanned for viruses based on the settings in the <email></email> XML tags. You can configure virus scanning for SMTP, POP3, and Microsoft Outlook.

```
<forticlient_configuration>
  <antivirus>
    <email>
      <smtp>1</smtp>
      <pop3>1</pop3>
      <outlook>1</outlook>
      <wormdetection>
        <enabled>0</enabled>
        <action>0</action>
      </wormdetection>
      <heuristic_scanning>
        <enabled>0</enabled>
        <action>0</action>
      </heuristic_scanning>
    </email>
  </antivirus>
</forticlient_configuration>
```

Table 22 provides email XML tags, the description, and the default value (where applicable).

Table 22: Email XML tags

XML Tag	Description	Default Value
<smtp>	When enabled, scan email messages sent through SMTP protocol. Boolean value: [0 | 1]	1
<pop3>	Determines whether to scan email messages received through POP3 protocol. Boolean value: [0 | 1]	1
<outlook>	Scan email files processed through Microsoft Outlook. Boolean value: [0 | 1]	1
<wormdetection> elements		
<enabled>	Scan for worm viruses. Boolean value: [0 | 1]	0

Table 22: Email XML tags (continued)

<action>	The action FortiClient will perform if a virus is found. Select either: • 0: warn • 1: terminate process	0
<heuristic_scanning> elements		
<enabled>	Enable or disable heuristics signatures. Boolean value: [0 | 1]	0
<action>	The action FortiClient will perform if a virus is found. Select either: • 0: log and warn • 1: strip and quarantine	0

Quarantine

The maximum age for quarantined files is specified in the <quarantine></quarantine> XML tags.

```
<forticlient_configuration>
  <antivirus>
    <quarantine>
      <cullage>100</cullage>
    </quarantine>
  </antivirus>
</forticlient_configuration>
```

Table 23 provides quarantine XML tag, the description, and the default value (where applicable).

Table 23: Quarantine XML tags

XML Tag	Description	Default Value
<cullage>	How long to hold quarantined files, in days, before deleting them. A number from 1 to 365.	100

Server

On Microsoft Windows servers, it may be desired to exclude system files from being scanned. These are configured in the <server></server> XML tags.

```
<forticlient_configuration>
  <antivirus>
    <server>
      <exchange>
        <integrate>0</integrate>
        <action>0</action>
        <excludefilesystemfromscanning>0</excludefilesystemfromsca
            nning>
        <excludefileextensionsfromscanning>0</excludefileextension
            sfromscanning>
    </exchange>
    <sqlserver>
        <excludefilesystemfromscanning>0</excludefilesystemfromsca
            nning>
        <excludefileextensionsfromscanning>0</excludefileextension
            sfromscanning>
      </sqlserver>
    </server>
  </antivirus>
</forticlient_configuration>
```

Table 24 provides server XML tags, the description, and the default value (where applicable).

Table 24: Server XML tags

XML Tag	Description	Default Value
<exchange> elements		
<integrate>	When the boolean value is set to 1 FortiClient integrates into Exchange Server. Boolean value: [0 | 1]	0
<action>	The action FortiClient will perform if a virus is found. Select either: • 0: Quarantine • 1: Remove Attachment Only	0
<excludefilesystemfromscanning>	Enable to exclude file system from scanning. Boolean value: [0 | 1]	0
<excludefileextensionsfromscanning>	Enable to exclude file extensions from scanning. Boolean value: [0 | 1]	0
<sqlserver> elements		

Table 24: Server XML tags (continued)

<excludefilesystemfromscanning>	Enable to exclude file system from scanning. Boolean value: [0 | 1]	0
<excludefileextensionsfromscanning>	Enable to exclude file extensions from scanning. Boolean value: [0 | 1]	0

Single Sign-On Mobility Agent

Configuration elements for FortiClient Single Sign-On Mobility Agent are contained in the <fssoma></fssoma> XML tags.

```
<forticlient_configuration>
  <fssoma>
    <enabled>0</enabled>
    <serveraddress>IP_or_FQDN</serveraddress>
    <presharedkey>Encypted_Preshared_Key</presharedkey>
  </fssoma>
</forticlient_configuration>
```

Table 25 provides Single Sign-On XML tags, the description, and the default value (where applicable).

Table 25: Single Sign-On XML tags

XML Tag	Description	Default Value
<enabled>	Enable or disable Single Sign On (SSO). Boolean value: [0 | 1]	0
<serveraddress>	FortiAuthenticator IP address or FQDN.	
<presharedkey>	Encrypted or unencrypted pre-shared key.	

To enable the FortiClient SSO Mobility agent service on the FortiAuthenticator, you must first apply the applicable FortiClient license for FortiAuthenticator. For more information, see the *FortiAuthenticator v3.0 Administration Guide* at http://docs.fortinet.com. For information on purchasing a FortiClient license, please contact your authorized Fortinet reseller.

WAN Optimization

WAN Optimization is configured in the <wan_optimization></wan_optimization> XML tags.

```
<forticlient_configuration>
  <wan_optimization>
    <enabled>0</enabled>
    <support_http>1</support_http>
    <support_cifs>1</support_cifs>
    <support_mapi>1</support_mapi>
    <support_ftp>1</support_ftp>
    <max_disk_cache_size_mb>512</max_disk_cache_size_mb>
  </wan_optimization>
</forticlient_configuration>
```

Table 26 provides WAN Optimization XML tags, the description, and the default value (if applicable).

Table 26:WAN Optimization XML tags

XML Tag	Description	Default Value
<enabled>	Enable or disable WAN Optimization. Boolean value: [0 | 1]	0
<support_http>	Enable or disable HTTP support. Boolean value: [0 | 1]	1
<support_cifs>	Enable or disable CIFS support. Boolean value: [0 | 1]	1
<support_mapi>	Enable or disable MAPI support. Boolean value: [0 | 1]	1
<support_ftp>	Enable or disable FTP support. Boolean value: [0 | 1]	1
<max_disk_cache_size_mb>	Maximum disk cache size in MB.	512

Web Filtering

Web Filtering XML configurations are contained in the <webfilter></webfilter> tags.

There are two main sections:

- General options

  Configuration elements that affect the whole of the web filtering service.
- Profiles

  Defines one or more rules that will be applied to network traffic.

```
<forticlient_configuration>
  <webfilter>
    <https_enabled>1</https_enabled>
    <enable_filter>1</enable_filter>
    <enabled>1</enabled>
    <log_all_urls>0</log_all_urls>
    <block_uncategorised>0</block_uncategorised>
    <white_list_has_priority>0</white_list_has_priority>
    <current_profile>0</current_profile>
    <partial_match_host>0</partial_match_host>
    <disable_when_managed>0</disable_when_managed>
    <max_violations>250</max_violations>
    <max_violations_age>7</max_violations_age>
    <profiles>
      <profile>
        <id>0</id>
        <cate_ver>6</cate_ver>
        <description>deny</descxription>
        <name>deny</name>
        <temp_whitelist_timeout>300</temp_whitelist_timeout>
        <categories>
          <fortiguard>
            <url>fgd1.fortigate.com</url>
            <enabled>1</enabled>
            <block_unrated>0</block_unrated>
            <rate_ip_addresses>1</rate_ip_addresses>
          </fortiguard>
          <category>
            <id>3</id>
            <action>deny</action>
          </category>
          <category>
            <id>4</id>
            <action>deny</action>
          </category>
          <category>
            <id>5</id>
            <action>deny</action>
          </category>
```

```
      </categories>
      <urls>
        <url>
          <address>www.playboy.com</address>
          <action>deny</action>
        </url>
          <address>www.fortinet.com</address>
          <action>allow</action>
        </url>
      </urls>
  </profile>
  <profile>
    <id>2</id>
    <cate_ver>6</cate_ver>
    <description>deny</description>
    <name>deny</name>
    <temp_whitelist_timeout>300</temp_whitelist_timeout>
    <categories>
        <fortiguard>
          <url>fgd1.fortigate.com</url>
          <enabled>1</enabled>
          <block_unrated>0</block_unrated>
          <rate_ip_addresses>1</rate_ip_addresses>
    </fortiguard>
      <category>
        <id>26</id>
        <action>deny</action>
      </category>
      <category>
        <id>86</id>
        <action>deny</action>
      </category>
    </categories>
    <safe_search>
      <enabled>1</enabled>
      <search_engines>
        <enabled>1</enabled>
        <engine>
          <name>bing</name>
          <host>
            <![CDATA[www\.bing\.com]]></host>
          <url>
            <![CDATA[^(\/images|\/videos)\/search]]></url>
          <query>
            <![CDATA[q=]]></query>
          <safe_search_string>
            <![CDATA[adlt=strict]]></safe_search_string>
          <cookie_name><![CDATA[]]</cookie_name>
          <cookie_value><![CDATA[]]</cookie_value>
```

```
            </engine>
            <engine>
               <name>yandex</name>
               <host>
                  <![CDATA[yandex\..*]]></host>
               <url>
                  <![CDATA[^\/yandsearch?\?]]></url>
               <query>
                  <![CDATA[text=]]></query>
               <safe_search_string>
                  <![CDATA[yandex=1]]></safe_search_string>
            </engine>
         </search_engines>
         <youtube_education_filter>
            <enabled>1</enabled>
               <filter_id>
                  <![CDATA[TkZEbkhj6lafXjw2-aQZcw]]></filter_id>
            </youtube_education_filter>
         </safe_search>
      </profile>
   </profiles>
</webfilter>
</forticlient_configuration>
```

Table 27 provides Web Filtering XML tags, the description, and the default value (where applicable).

Table 27: Web Filtering XML tags

XML Tag	Description	Default Value
<https_enabled>	Enable or disable Web Filtering on HTTPS traffic. Boolean value: [0 | 1]	1
<enable_filter>	Enable or disable Web Filtering. Boolean value: [0 | 1]	1
<enabled>	Enable or disable FortiGuard querying service. Boolean value: [0 | 1]	1
<log_all_urls>	Record all visited URLs to the log file, both blocked and allowed. Boolean value: [0 | 1]	0
<block_uncategorised>	Block network traffic that does not match any rules. Boolean value: [0 | 1]	0
<white_list_has_priority>	If traffic matches both a block and an allow rule, it should be allowed. Boolean value: [0 | 1]	0
<current_profile>	Currently selected profile ID. (optional)	

Table 27: Web Filtering XML tags (continued)

<partial_match_host>	A hostname that is a substring of the specified path is treated as a full match. Boolean value: [0 | 1]	0
<disable_when_managed>	If set to 1 (true), Web Filtering will be disabled when FortiClient is registered to a FortiGate using Endpoint Control. Boolean: [0 | 1]	
<max_violations>	Maximum number of violations stored at any one. A number from 250 to 5000.	5000
<max_violation_age>	Maximum age in days of a violation record before it is culled. A number from 1 to 90.	90
<fortiguard> elements		
<url>	IP address or FQDN of the FortiGuard server.	fgd1.fortigate.com
<enabled>	Enable or disable use of FortiGuard servers. Boolean value: [0 | 1]	1
<block_unrated>	Block unrated URLs. Boolean value: [0 | 1]	0
<rate_ip_addresses>	Rate IP addresses. Boolean value: [0 | 1]	1
<profiles><profile><safe_search> element		
<enabled>	Enable or disable SafeSearch. Boolean value: [0 | 1]	
<profiles><profile><safe_search><search_engines><engine> element		
<enabled>	Enable or disable SafeSearch for the predefined search engines. Boolean value: [0 | 1]	

The <profiles> XML element may have one or more profiles, defined in the <profile> tag. Each <profile>, in turn, has one or more <category>, <url> and <safe_search> tags, along with other elements.

Table 28 provides profile XML tags, the description, and the default value (where applicable).

Table 28: Profile XML tags

XML Tag	Description	Default Value
<profile> elements		

Table 28: Profile XML tags (continued)

<id>	Unique ID. A number to define the profile.	
<cate_ver>	FortiGuard category version used in this profile. A number.	6
<description>	Summary describing this profile.	
<name>	A descriptive name for the profile.	
<temp_whitelist_timeout>	The duration, in seconds, of a bypass that is applied to a page that generated a *warning*, but for which the user selected *continue*.	300
<profile><categories><category> elements		
<id>	Unique ID. A number. The valid set of category IDs is predefined, and is listed in exported configuration files.	
<action>	Action to perform on matching network traffic. Select one of the following: • allow • deny • warn • monitor	
<profile><urls><url> elements		
<address>	The web address in which <action> (allow or deny) will be performed. This should be wrapped in a CDATA tag. For example: <![CDATA[www.777.com]]>	
<action>	Action to perform on matching network traffic. Select either: [allow | deny]	

The <safe_search> element has two main components:

- Search engines <search_engines>

  Users may define safe search parameters for each of the popular search engines: Bing and Yandex. Subsequent use of the engines for web searches will have SafeSearch enabled.
- YouTube education filter <youtube_education_filter>

Educational institutions with valid YouTube education ID can provide this in the <youtube_education_filter> element to restrict YouTube contents appropriately.

Table 29 provides profile XML tags and the description. See the <safe_search> listing in the previous pages for examples of each tag.

Table 29: Profile XML tags

XML Tag	Description	Default Value
<profiles><profile><safe_search><search_engines><engine> elements		
<name>	Name of the SafeSearch profile.	
<host>	The FQDN of the search engine. FortiClient will monitor attempts to visit this address.	
<url>	The URL substring to match or monitor, along with the FQDN.	
<query>	The query string that will be appended to the URL.	
<safe_search_string>	The correct safe search string that will be appended to the URL for the specified engine.	
<cookie_name>	The name of the cookie to send the search engine.	
<cookie_value>	The cookie value to send the search engine.	
<profiles><profile><safe_search><youtube_education_filter> elements		
<enabled>	Enable YouTube education filter. Boolean value: [0 | 1]	
<filter_id>	The institutions education identifier.	

Other than the <name> and <enabled> elements, the values for each of the elements in the previous table should be wrapped in <![CDATA[]]> XML tags. Here is an example for a <host> element taken from the <safe_search> listing.

```
<host><![CDATA[yandex\..*]]></host>
```

See http://support.google.com/youtube/bin/answer.py?hl=en&answer=2592715 for more information on YouTube for schools and the education filter.

The following is a list of all Web Filter categories including the category <id> and category name:

```
0 ==> Unrated
1 ==> Drug Abuse
2 ==> Alternative Beliefs
3 ==> Hacking
4 ==> Illegal or Unethical
5 ==> Discrimination
6 ==> Explicit Violence
7 ==> Abortion
8 ==> Other Adult Materials
9 ==> Advocacy Organizations
11 ==> Gambling
12 ==> Extremist Groups
13 ==> Nudity and Risque
```

```
14 ==> Pornography
15 ==> Dating
16 ==> Weapons (Sales)
17 ==> Advertising
18 ==> Brokerage and Trading
19 ==> Freeware and Software Downloads
20 ==> Games
23 ==> Web-based Email
24 ==> File Sharing and Storage
25 ==> Streaming Media and Download
26 ==> Malicious Websites
28 ==> Entertainment
29 ==> Arts and Culture
30 ==> Education
31 ==> Finance and Banking
33 ==> Health and Wellness
34 ==> Job Search
35 ==> Medicine
36 ==> News and Media
37 ==> Social Networking
38 ==> Political Organizations
39 ==> Reference
40 ==> Global Religion
41 ==> Search Engines and Portals
42 ==> Shopping and Auction
43 ==> General Organizations
44 ==> Society and Lifestyles
46 ==> Sports
47 ==> Travel
48 ==> Personal Vehicles
49 ==> Business
50 ==> Information and Computer Security
51 ==> Government and Legal Organizations
52 ==> Information Technology
53 ==> Armed Forces
54 ==> Dynamic Content
55 ==> Meaningless Content
56 ==> Web Hosting
57 ==> Marijuana
58 ==> Folklore
59 ==> Proxy Avoidance
61 ==> Phishing
62 ==> Plagiarism
63 ==> Sex Education
64 ==> Alcohol
65 ==> Tobacco
66 ==> Lingerie and Swimsuit
67 ==> Sports Hunting and War Games
68 ==> Web Chat
```

```
69 ==> Instant Messaging
70 ==> Newsgroups and Message Boards
71 ==> Digital Postcards
72 ==> Peer-to-peer File Sharing
75 ==> Internet Radio and TV
76 ==> Internet Telephony
77 ==> Child Education
78 ==> Real Estate
79 ==> Restaurant and Dining
80 ==> Personal Websites and Blogs
81 ==> Secure Websites
82 ==> Content Servers
83 ==> Child Abuse
84 ==> Web-based Applications
85 ==> Domain Parking
86 ==> Spam URLs
87 ==> Personal Privacy
```

Application Firewall

Application Firewall configuration data is contained in `<firewall></firewall>` XML tags.

The set of elements may be grouped into two:

- General options

  Options that apply to the entire firewall activities.
- Profiles

  Defines the applications and the actions to apply to them.

```
<forticlient_configuration>
  <firewall>
    <enabled>1</enabled>
    <current_profile>0</current_profile>
    <default_action>Pass</default_action>
    <show_bubble_notifications>0</show_bubble_notifications>
    <max_violations>250</max_violations>
    <max_violations_age>7</max_violations_age>
    <profiles>
      <profile>
        <id>0</id>
        <rules>
          <rule>
            <action>Block</action>
            <enabled>1</enabled>
            <application>
              <id>16783</id>
            </application>
        </rule>
          <rule>
            <action>Block</action>
```

```
                <enabled>1</enabled>
                <category>
                <id>2</id>
                </category>
              </rule>
            </rules>
          </profile>
        </profiles>
      </firewall>
    </forticlient_configuration>
```

Table 30 provides Application Firewall XML tags, the description, and the default value (where applicable).

Table 30: Application Firewall XML tags

XML Tag	Description	Default Value
<enabled>	Enable or disable Application Firewall. Boolean value: [0 | 1]	1
<current_profile>	Currently selected profile ID.	
<default_action>	Action to enforce on traffic that does not match any of the profiles defined. Select one of the following: • block • reset • pass	pass
<show_bubble_notifications>	Display a bubble message each time an application is blocked for matching a profile. Boolean value: [0 | 1]	
<max_violations>	Maximum number of violations stored at any one. A number from 250 to 5000	5000
<max_violation_age>	Maximum age in days of a violation record before it is culled. A number from 1 to 90.	90

The <profiles> tag may contain one or more <profile> tags, each of which has a <rules> element. The <rules> element may, itself, have zero or more <rule> tags.

The following filter elements may be used to define applications in a <rule> tag:

```
<category>
<vendor>
<behavior>
<technology>
<protocol>
<application>
<popularity>
```

If the <application> element is present, all other sibling elements (listed above) will be ignored. If it is not, a given application must match all of the provided filters to trigger the rule.

Each of these seven elements is a container for the tag: <ids>, which is a list of the identifiers (numbers) selected for that particular filter. The full <firewall> profile listed at the beginning of this section shows several examples of the use of filters within the <rule> element. Using an <ids> value all will select all matching applications.

Table 31 provides profile element XML tags, the description, and the default value (where applicable).

Table 31: Profile element XML tags

XML Tag	Description	Default Value
<profile> element		
<id>	Unique ID. A unique ID number.	
<profile><rules><rule> elements		
<action>	Action to enforce on traffic that matches this rule. Select one of the following: • block • reset • pass	
<enabled>	Enable or disable this rule. Boolean value: [0 | 1]	1
<category>	Categories of the applications to apply <action> on.	csv list
<vendor>	Vendors of the applications to apply <action> on.	csv list
<behavior>	Behavior of the applications to apply <action> on.	csv list
<technology>	Technologies used by the applications to apply <action> on.	csv list
<protocol>	Protocols used by the applications to apply <action> on.	csv list
<application>	Identifiers (IDs) of the applications to apply <action> on.	csv list
<popularity>	Popularity of the applications to apply <action> on.	csv list

Vulnerability Scan

Configurations for Vulnerability Scan are contained in the <vulnerability_scan></vulnerability_scan> XML tags.

```
<forticlient_configuration>
  <vulnerability_scan>
    <enabled>1</enabled>
    <scan_on_fgt_registration>0</scan_on_fgt_registration>
    <scheduled_scans>
      <schedule>
        <enable_schedule>0</enable_schedule>
        <repeat>0</repeat>
        <type>24</type>
        <day>3</day>
        <time>19:30</time>
      <schedule>
    </scheduled_scans>
  </vulnerability_scan>
</forticlient_configuration>
```

Table 32 provides Vulnerability Scan XML tags, the description, and the default value (where applicable).

Table 32: Vulnerability Scan XML tags

XML Tag	Description	Default Value
<enabled>	Vulnerability Scan is enabled.	
<scan_on_fgt_registration>	Scan system on FortiGate registration. Boolean value: [0 | 1]	0
<scheduled_scans><schedule> elements Currently there can only be one scheduled item.		
<enable_schedule>	Enable or disable schedule. Boolean value: [0 | 1]	
<repeat>	Frequency of scans. Select one of the following: • 0: daily • 1: weekly • 2: monthly	
<type>	Type of vulnerability scan. Select one of the following: • 8: high • 16: critical • 24: high & critical	24

Table 32: Vulnerability Scan XML tags (continued)

<day>	If the <repeat> tag is set to 0 (daily), the <day> tag is ignored. If the <repeat> tag is set to 1 (weekly), <day> is the day of the week to run scan. Select one of the following: • 1: Sunday • 2: Monday • 3: Tuesday • 4: Wednesday • 5: Thursday • 6: Friday • 7: Saturday If the <repeat> tag is set to 2 (monthly), <day> is the day of the month to run a scan. A number from 1 to 31.	The default is the date the policy was installed from the FortiGate.
<time>	Time value in 24 hour clock.	The default is the time the policy was installed from the FortiGate.

FortiClient XML Configurations

The FortiClient configuration file is user editable. The file uses XML format for easy parsing and validation. The configuration file is inclusive of all client configurations, and references the client certificates.

Design considerations

Input validation

The import function performs basic validation, and writes to log when errors or warnings are found. Default values for omitted items are defined for VPN connections. For other settings omitted values are ignored.

Handling of password fields

When exporting, the password and username fields will be encrypted (prefixed with “Enc”). However, the import function is able to take either the clear text or encrypted format.

Segment of configuration file

It is valid to import the segment of a configuration file. However, the segment should follow the syntax and level defined in this document. For example, this is a valid segment:

```
<?xml version=”1.0” encoding=”utf-8”?>
<forticlient_configuration>
  <VPN>
    <SSLVPN>
      <connections>
        <connection>
          // connection 1
        </connection>
      </connections>
    </SSLVPN>
  </VPN>
</forticlient_configuration>
```

This is not a valid segment:

```
<?xml version=”1.0” encoding=”utf-8”?>
  <connections>
    <connection>
      // connection 1
    </connection>
  </connections>
```

Client certificate

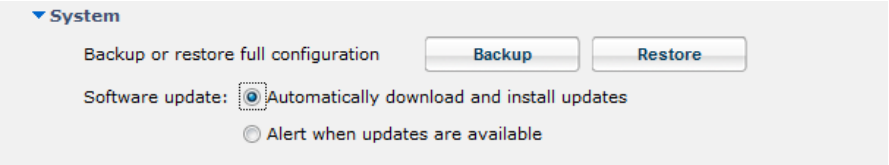
The configuration file will include the client certificate(s) when exported in an encrypted format.

Backup or Restore the Configuration File

Backup the full configuration file

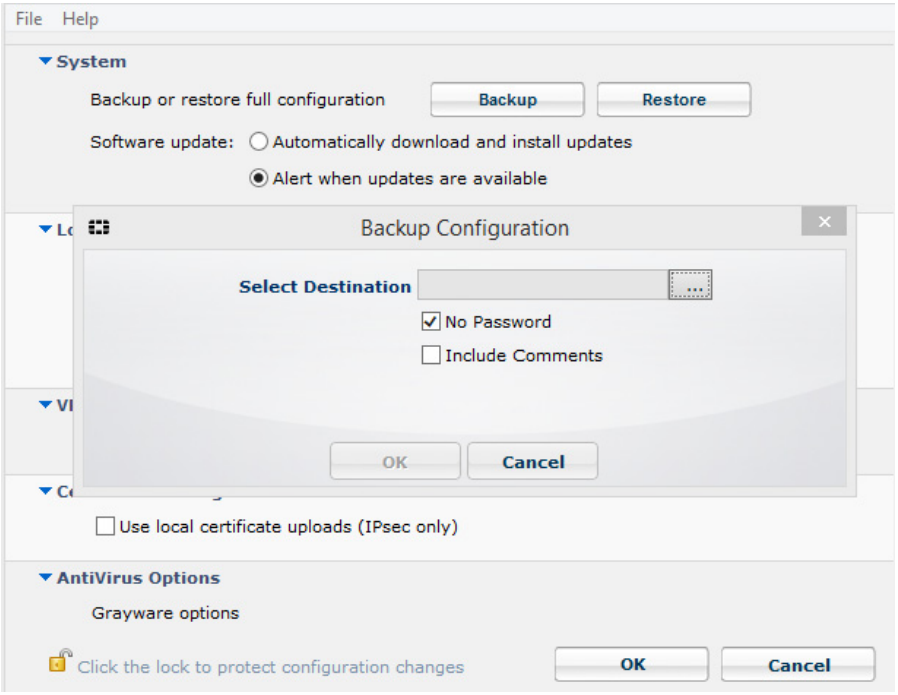
To backup the full configuration file, select *File* on the toolbar, and *Settings* on the drop-down menu. Select *System* to view the drop-down menu. On this menu you can perform a backup of the full configuration file.

Figure 1: Backup and Restore options



When performing a backup, you can select the file destination, and save the file in an unencrypted or encrypted format. To encrypt the configuration file enter a password. When selecting No Password, you can also select to include comments in the configuration file.

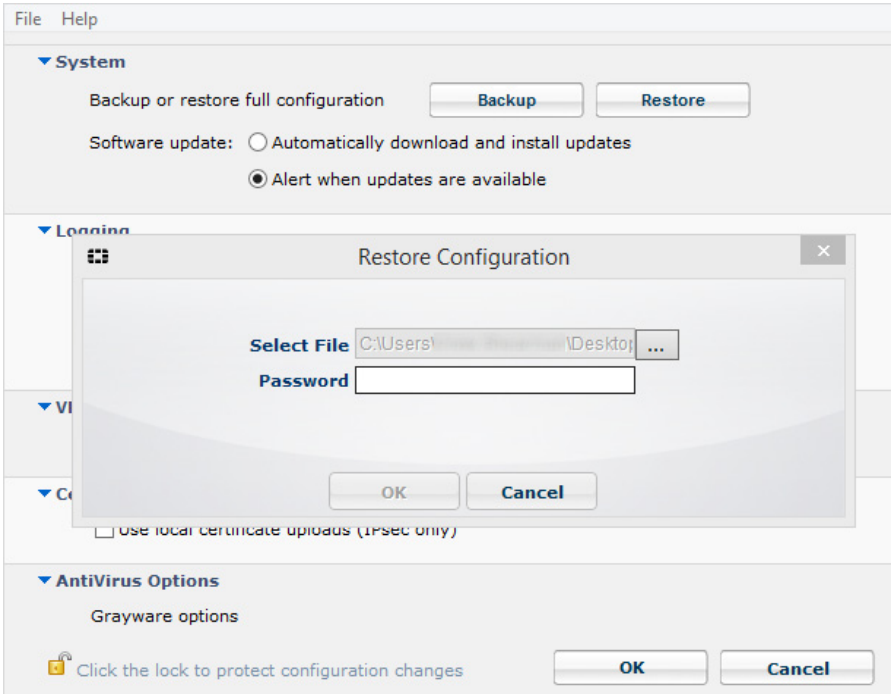
Figure 2: Backup configuration file options



Restore the full configuration file

To restore a full configuration file, select *File* on the toolbar, and *Settings* on the drop-down menu. Select *System* to view the drop-down menu. On this menu you can select *Restore* to import a backup of the full configuration file. Select *Restore* and browse for the file on your local hard disk drive.

Figure 3: Restore a configuration file



If the configuration was protected with a password, a password textbox will be displayed. Enter the password used to encrypt the backup configuration file.

Backup and restore command line utility commands and syntax

Fortinet provides administrators the ability to import and export configurations via the CLI. The fcconfig utility can be run locally or remotely as the system user (or admin user) to import or export the configuration file. In Microsoft Windows, the fcconfig utility is located in the C:\Program Files (x86)\Fortinet\FortiClient> directory. In Mac OS X, the fccconfig utility is located in the /Library/Application Support/Fortinet/FortiClient/bin directory.

The following commands are available for use:

Backup the configuration file

```
FCConfig -m all -f <filename> -o export -i 1
```

Backup the configuration file (encrypted)

```
FCConfig -m all -f <filename> -o export -i 1 -p <encrypted password>
```

Restore the configuration file

```
FCConfig -m all -f <filename> -o import -i 1
```

Restore the configuration file (encrypted)

```
FCConfig -m all -f <filename> -o import -i 1 -p <encrypted password>
```

Export the VPN tunnel configuration

```
FCConfig -m vpn -f <filename> -o exportvpn -i 1
```

Export the VPN tunnel configuration (encrypted)

```
FCConfig -m vpn -f <filename> -o exportvpn -i 1 -p <encrypted
    password>
```

Import the VPN tunnel configuration

```
FCConfig -m vpn -f <filename> -o importvpn -i 1
```

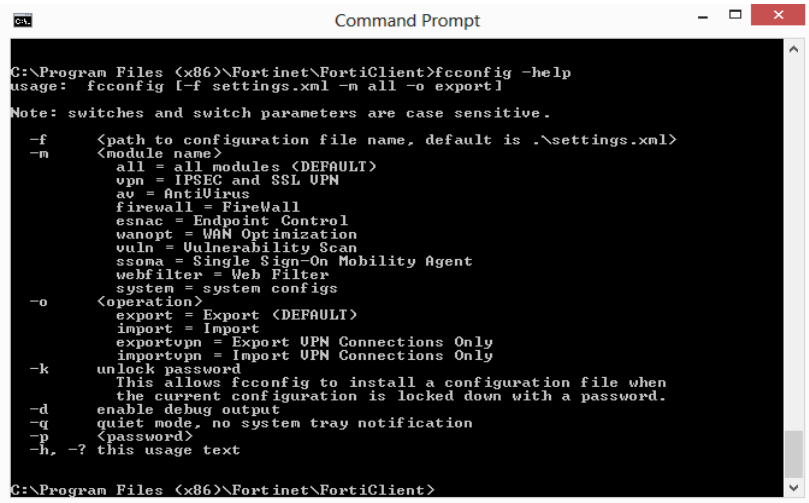
Import the VPN tunnel configuration (encrypted)

```
FCConfig -m vpn -f <filename> -o importvpn -i 1 -p <encrypted
    password>
```

Switches and switch parameters are case sensitive.

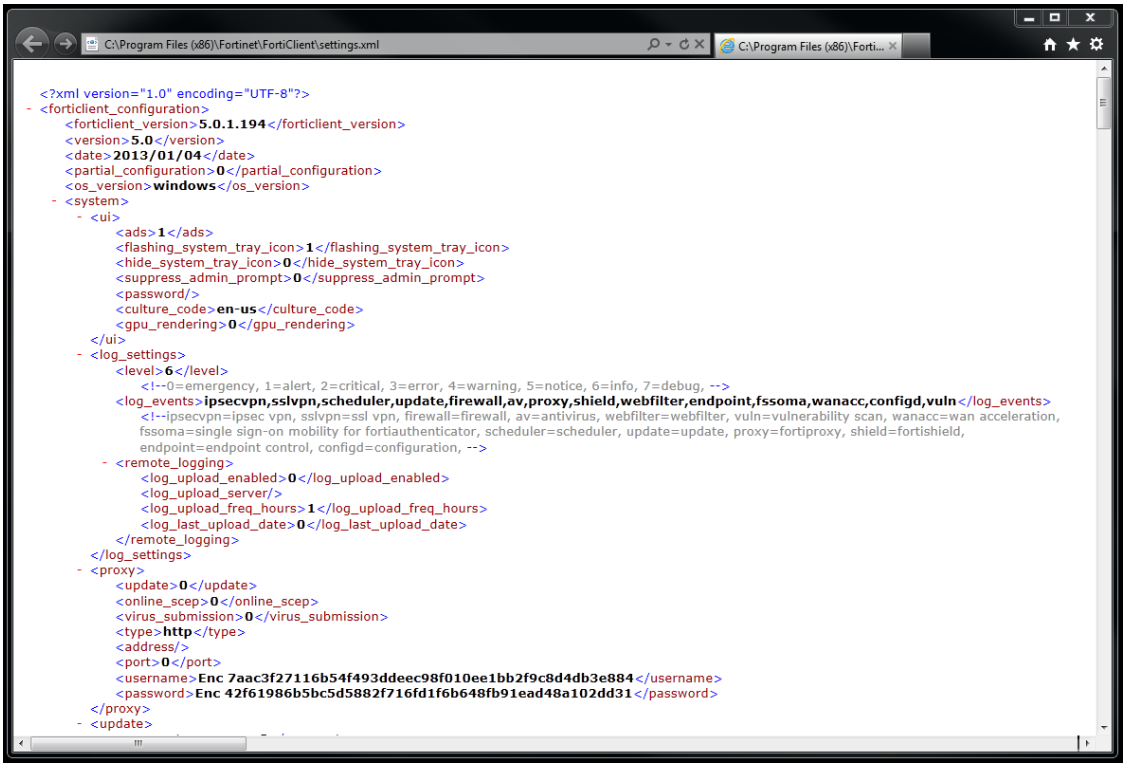
Backup and restore CLI commands are an advanced configuration option.

Figure 4: Administrative command prompt



The command `fccconfig -f settings.xml -m all -o export` will export the configuration as XML file in the FortiClient directory. See Figure 5 for an XML configuration example.

Figure 5: Exported XML configuration example



Upload the FortiClient XML file to FortiGate

In FortiOS v5.0.0 or later, the buffer size for the FortiClient Profile XML configuration is 32kB. When `set forticlient-advanced-cfg enable` is enabled, you can cut & paste FortiClient XML elements into the FortiGate FortiClient Profile.

To deploy the full XML configuration via the FortiClient Profile:

1. Log in to the FortiGate Command-line Interface.
2. Enter the following CLI commands:

```
config endpoint-control profile
  edit <profile_name>
  config forticlient-winmac-settings
    set forticlient-advanced-cfg enable
    set forticlient-advanced-cfg-buffer "Copy & Paste your
        FortiClient XML configuration here"
  end
end
```

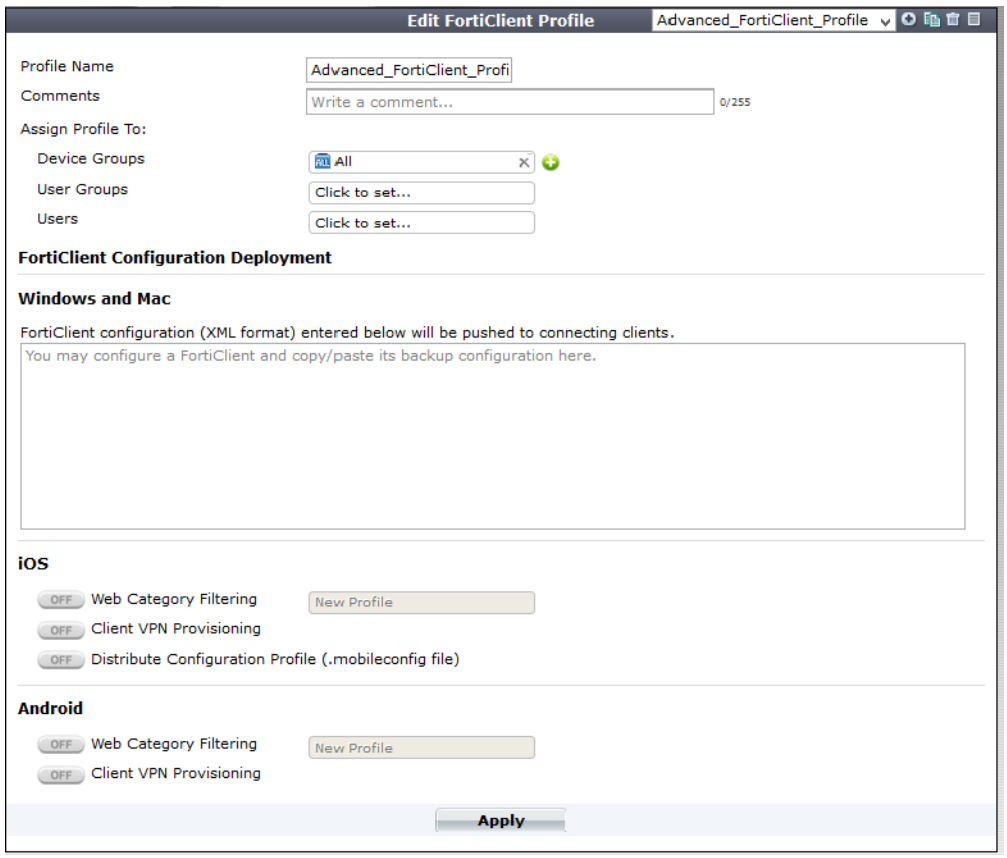
After `forticlient-advanced-cfg` is enabled, the `forticlient-advanced-cfg-buffer` CLI command is available from the CLI.

Copy directly from your XML editor, preserving the XML file format. Copy all information from the `<?xml version="1.0" encoding="UTF-8" ?>` start of syntax to the `</forticlient_configuration>` end of syntax XML tags. Add double quotes at the start and end of the XML syntax statements.

The buffer size for the FortiClient Profile XML configuration is 32kB.

You can also choose to copy & paste the XML content in the Web-based Manager, go to *User & Device* > *Endpoint Protection* > *FortiClient Profiles.*

Figure 6: Advanced FortiClient Profile



Configure the following settings:

Profile Name	Enter a unique name to identify the FortiClient Profile.
Comments	Optionally, enter a comment.
Assign Profile To	For more information on configuring device groups, user groups, and users, see the *FortiOS 5.0 Handbook*. Note: These options are only available when creating a new endpoint profile. Note: You can assign the profile to user groups and users when using Active Directory authentication or RADIUS authentication for VPN.
Device Groups	Select device groups from the drop down-menu. Use the plus (+) icon to select more than one device group.
User Groups	Select user groups from the drop-down menu. Use the plus (+) icon to select more than one device group.
Users	Select users from the drop-down menu. Use the plus (+) icon to select more than one device group.

FortiClient Configuration Deployment Windows and Mac	
XML text window	Cut and paste the FortiClient XML configuration file in the text window. The XML syntax must be preserved.

Select *Apply* to save the endpoint profile settings.

To provision specific FortiClient XML configuration while preserving custom XML configurations in your MSI file, cut & paste the specific XML configuration into the FortiClient Profile in the following format:

```
<?xml version="1.0" encoding="UTF-8" ?>
<forticlient_configuration>
  <partial_configuration>1</partial_configuration>
  <system>
    <ui>
      <ads>0</ads>
      <default_tab>VPN</default_tab>
      <flashing_system_tray_icon>0</flashing_system_tray_icon>
      <hide_system_tray_icon>0</hide_system_tray_icon>
      <suppress_admin_prompt>0</suppress_admin_prompt>
      <culture_code>os-default</culture_code>
    </ui>
    <update>
      <use_custom_server>0</use_custom_server>
      <port>80</port>
      <timeout>60</timeout>
      <failoverport>8000</failoverport>
      <fail_over_to_fdn>1</fail_over_to_fdn>
      <scheduled_update>
        <enabled>0</enabled>
        <type>interval</type>
        <daily_at>03:00</daily_at>
        <update_interval_in_hours>3</update_interval_in_hours>
    </scheduled_update>
    </update>
  </system>
</forticlient_configuration>
```

Ensure that the `<partial_configuration>1</partial_configuration>` tag is set to 1 to indicate that this partial configuration will be deployed upon registration with the FortiGate. All other XML configuration will be preserved.

Advanced VPN provisioning

You need to enable VPN provisioning and advanced VPN from the FortiOS CLI to import the FortiClient XML VPN configuration syntax. You can import the XML VPN configuration in the CLI or the Web-based Manager.

Import XML VPN configuration into the FortiClient Profile via the CLI:

1. Log in to your FortiGate command-line interface.
2. Enter the following CLI commands:

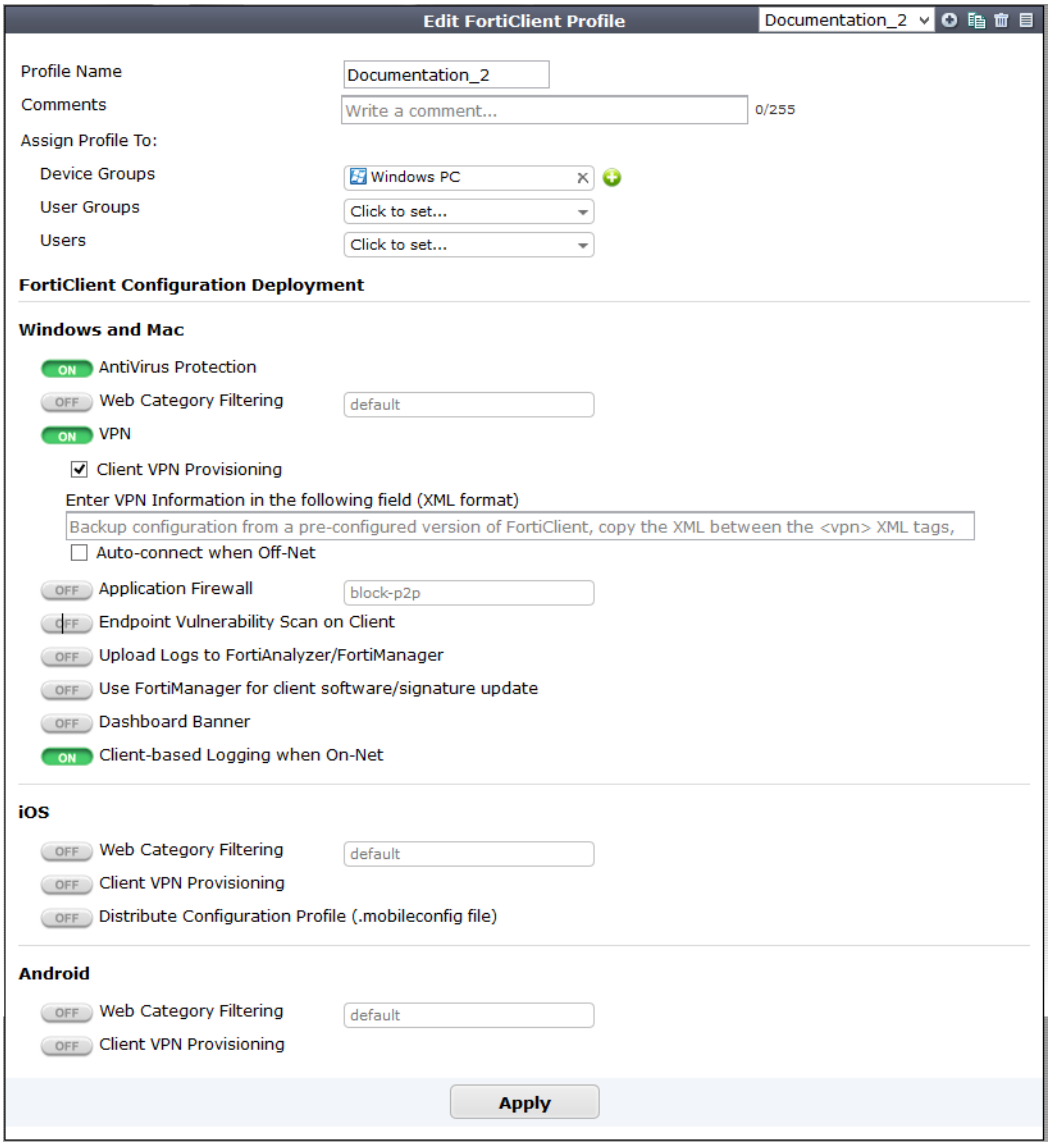
```
config endpoint-control profile
  edit <profile_name>
  config forticlient-winmac-settings
    set forticlient-vpn-provisioning enable
    set forticlient-advanced-vpn enable
    set forticlient-advanced-vpn-buffer "Copy & paste the
        advanced VPN configuration"
  end
end
```

After the `forticlient-vpn-provisioning` and `forticlient-advanced-vpn` CLI commands are enabled, the `forticlient-advanced-vpn-buffer` CLI command is available from the CLI.

Copy directly from your XML editor, preserving the XML file format. Copy all information from the `<vpn>` start of syntax to the `</vpn>` end of syntax XML tags. Add double quotes before the <vpn> tag and after the </vpn> tag.

You can also choose to copy & paste the XML content in the Web-based Manager, go to *User & Device* > *Endpoint Protection* > *FortiClient Profiles.*

Figure 7: Advanced FortiClient Profile (VPN)



Configure the following settings:

Profile Name	Enter a unique name to identify the FortiClient Profile.
Comments	Optionally, enter a comment.
Assign Profile To	For more information on configuring device groups, user groups, and users, see the *FortiOS Handbook*. Note: These options are only available when creating a new endpoint profile. Note: You can assign the profile to user groups and users when using Active Directory authentication or RADIUS authentication for VPN.
Device Groups	Select device groups from the drop down-menu. Select the add icon, , to select more than one device group.

User Groups	Select user groups from the drop-down menu. Select the add icon,  , to select more than one device group.
Users	Select users from the drop-down menu. Select the add icon,  , to select more than one device group.
FortiClient Configuration Deployment Windows and Mac	
AntiVirus Protection	Toggle the button on or off to enable or disable this feature.
Web Category Filtering	Toggle the button on or off to enable or disable this feature. When enabled, you can select a web filter profile in the drop-down menu. Select the checkbox to disable web category filtering on the client when protected by the FortiGate.
VPN	Select the checkbox for Client VPN Provisioning. Cut and paste the FortiClient XML configuration <vpn> to </vpn> tags in the text window. The XML syntax must be preserved. Select the checkbox to autoconnect when the client is off-net.
Application Firewall	Toggle the button on or off to enable or disable this feature. When enabled, you can select an application control sensor in the drop-down menu.
Endpoint Vulnerability Scan on Client	Toggle the button on or off to enable or disable this feature. When enabled, you can select the scheduled scan type to daily, weekly, or monthly. Select the checkbox to initiate a scan after client registration with the FortiGate.
Upload Logs to FortiAnalyzer/FortiManager	Toggle the button on or off to enable or disable this feature. When enabled, you can select to use the same FortiAnalyzer/FortiManager used by the FortiGate or select Specify to enter a different device IP. You can set the schedule to hourly or daily. The FortiClient upload logs to the FortiAnalyzer/FortiManager only when it is able to connect to the device on the specified IP address.
Use FortiManager for client software/signature update	Toggle the button on or off to enable or disable this feature. When enabled, you can specify the IP address of the FortiManager. Select the checkbox to failover to the FortiGuard Distribution Network (FDN) when the FortiManager is not available.

Dashboard Banner	Toggle the button on or off to enable or disable this feature.
Client-based Logging when On-net	Toggle the button on or off to enable or disable this feature.

Select *Apply* to save the FortiClient Profile settings.

Advanced Features

Advanced features (Windows)

Connect VPN before logon (AD environments)

The VPN `<options>` XML tag holds global information controlling VPN states. The VPN will connect first, then logon to AD/Domain.

```
<forticlient_configuration>
  <vpn>
    <options>
      <show_vpn_before_logon>1</show_vpn_before_logon>
      <use_windows_credentials>1</use_windows_credentials>
    </options>
  </vpn>
</forticlient_configuration>
```

Create a redundant IPsec VPN

To use VPN resiliency/redundancy, you will configure a list of FortiGate IP/FQDN servers, instead of just one:

```
<forticlient_configuration>
  <vpn>
    <ipsecvpn>
        <options>
        ...
        </options>
          <connections>
            <connection>
              <name>psk_90_1</name>
              <type>manual</type>
              <ike_settings>
              <prompt_certificate>0</prompt_certificate>
              <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61
                  .143</server>
              <redundantsortmethod>1</redundantsortmethod>
              ...
          </ike_settings>
        </connection>
      </connections>
    </ipsecvpn>
  </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the IPsec VPN configuration are committed.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response based. The VPN will connect to the FortiGate which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0, and the IPsec VPN connection is priority based. Priority based configurations will try to connect to the FortiGate starting with the first on the list.

Priority based SSL VPN connections

SSL VPN supports priority based configurations for redundancy.

```
<forticlient_configuration>
  <vpn>
    <sslvpn>
      <options>
        <enabled>1</enabled>
        ...
      </options>
      <connections>
        <connection>
          <name>ssl_90_1</name>
          <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:44
              3</server>
          ...
        </connection>
      </connections>
    </sslvpn>
  </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are committed.

For SSL VPN, all FortiGates must use the same TCP port.

Enabling VPN autoconnect

VPN auto connect uses the following XML tag:

```
<autoconnect_tunnel>ipsecdemo.fortinet.com</autoconnect_tunnel>
```

Inside:

```
<vpn>
  <options>
```

Save password is also needed because it is autoconnect:

```
<save_password>1</save_password>
```

Enabling VPN always up

VPN always up uses the following XML tag:

```
<keep_running>1</keep_running>
```

Inside:

```
<vpn>
  <connection>
```

Advanced features (Mac OS X)

Create a redundant IPsec VPN

To use VPN resiliency/redundancy, you will configure a list of FortiGate IP/FQDN servers, instead of just one:

```
<forticlient_configuration>
  <vpn>
    <ipsecvpn>
        <options>
        ...
        </options>
          <connections>
            <connection>
              <name>psk_90_1</name>
              <type>manual</type>
              <ike_settings>
              <prompt_certificate>0</prompt_certificate>
              <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61
                  .143</server>
              <redundantsortmethod>1</redundantsortmethod>
              ...
          </ike_settings>
        </connection>
      </connections>
    </ipsecvpn>
  </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the IPsec VPN configuration are committed.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response based. The VPN will connect to the FortiGate which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0, and the IPsec VPN connection is priority based. Priority based configurations will try to connect to the FortiGate starting with the first on the list.

Priority based SSL VPN connections

SSL VPN supports priority based configurations for redundancy.

```
<forticlient_configuration>
  <vpn>
    <sslvpn>
      <options>
        <enabled>1</enabled>
        ...
      </options>
      <connections>
        <connection>
          <name>ssl_90_1</name>
          <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:44
              3</server>
          ...
        </connection>
      </connections>
    </sslvpn>
  </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are committed.

For SSL VPN, all FortiGates must use the same TCP port.

Enabling VPN autoconnect

VPN auto connect uses the following XML tag:

```
<autoconnect_tunnel>ssl 198 no cert</autoconnect_tunnel>
```

Enabling VPN always up

VPN always up uses the following XML tag:

```
<keep_running>1</keep_running>
```

VPN before logon is currently not supported in FortiClient v5.0 Patch Release 1 (Mac OS X).

VPN tunnel & script (Microsoft Windows)

Feature overview

This feature supports auto running a user-defined script after the configured VPN tunnel is connected or disconnected. The scripts are batch scripts in Windows and shell scripts in Mac OS X. They will be defined as part of a VPN tunnel configuration on FortiGate's XML format Endpoint Profile. The profile will be pushed down to FortiClient from FortiGate. When FortiClient's VPN tunnel is connected or disconnected, the respective script defined under that tunnel will be executed. These scripts can also be configured directly on FortiClient, by importing the XML configuration file.

Map a network drive after tunnel connection

The script will map a network drive and copy some files after the tunnel is connected.

```
<on_connect>
  <script>
    <os>windows</os>
      <script>
        <script>
          <![CDATA[
net use x: \\192.168.10.3\ftpshare /user:Honey Boo Boo
md c:\test
copy x:\PDF\*.* c:\test
              ]]>
        </script>
      </script>
  </on_connect>
```

Delete a network drive after tunnel is disconnected

The script will delete the network drive after the tunnel is disconnected.

```
<on_disconnect>
  <script>
    <os>windows</os>
    <script>
      <script>
        <![CDATA[
net use x: /DELETE
          ]]>
</script>
      </script>
    </script>
  </on_disconnect>
```

VPN tunnel & script (Mac OS X)

Map a network drive after tunnel connection

The script will map a network drive and copy some files after the tunnel is connected.

```
<on_connect>
  <script>
    <os>mac</os>
    <script>
      /bin/mkdir /Volumes/installers
      /sbin/ping -c 4 192.168.1.147 >
           /Users/admin/Desktop/dropbox/p.txt
      /sbin/mount -t smbfs
           //kimberly:RigUpTown@ssldemo.fortinet.com/installer
           s /Volumes/installers/ >
           /Users/admin/Desktop/dropbox/m.txt
      /bin/mkdir /Users/admin/Desktop/dropbox/dir
      /bin/cp /Volumes/installers/*.log
           /Users/admin/Desktop/dropbox/dir/.
    </script>
  </script>
</on_connect>
```

Delete a network drive after tunnel is disconnected

The script will delete the network drive after the tunnel is disconnected.

```
<on_disconnect>
  <script>
    <os>mac</os>
    <script>
      /sbin/umount /Volumes/installers
      /bin/rm -fr /Users/admin/Desktop/dropbox/*
  </script>
  </script>
</on_disconnect>
```

Index

S

U

V

W

X